Univerzita Karlova v Praze
Filozofická fakulta
Ústav informačních studií a knihovnictví

Studijní program: Informační studia a knihovnictví
Studijní obor: Informační studia a knihovnictví

Bc. Tomáš Rejnek

Přínosy a problémy využití cloud computingu ve státní správě, informačních institucích a knihovnách

Cloud Computing in Public Sector - Benefits and Risks

Diplomová práce

Praha 2015

Vedoucí práce: PhDr. Helena Lipková, Ph.D.

Prohlašuji, že jsem diplomovou práci vypracoval samostatně, že jsem řádně citoval všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 17. dubna 2015

Bc. Tomáš Rejnek

Identifikační záznam:

REJNEK, Tomáš. *Přínosy a problémy využití cloud computingu ve státní správě, informačních institucích a knihovnách = Cloud Computing in Public Sector - Benefits and Risks.* Praha, 2015-04-17. Diplomová práce (Mgr.). Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí diplomové práce Helena Lipková.

Abstrakt (česky)

Diplomová práce se zabývá přinosy a riziky využití cloud computingu institucemi veřejného sektoru. Práce se zaměřuje především na služby tzv. veřejného cloudu.

Práce je rozdělena do 4 hlavních částí. První část se věnuje definici a popisu základních vlastností cloud computingu. V druhé části práce je provedena PESTL analýza zkoumající vlivy makrookolí (konkrétně vlivy politické, ekonomické, sociální, technologické a legislativní) na využití cloud computingu institucemi veřejného sektoru. V třetí části práce byla vytvořena SWOT analýza zkoumající silné a slabé stránky cloudových technologií a možná hrozby a pří-ležitosti pro jejich využití v institucích veřejného sektoru. Poslední část práce představuje případovou studii využití cloud computingu na Filosofické fakultě Univerzity Karlovy v Praze.

Výsledky provedených analýz se kloní k pozitivním přínosům cloud computingu pro instituce veřejného sektoru za předpokladu, že provedou patřičnou přípravu a nepodcení rizika popsaná v této práci.

Klíčová slova (česky):
Cloud computing, IaaS, PaaS, SaaS, veřejný sektor, PESTL, SWOT, virtualizace

Abstrakt (anglicky)

This thesis deals with benefits and risks of using cloud computing in public sector institutions. The thesis focuses mainly on the usage of public cloud deployment model.

The thesis is divided into 4 main chapters. The first chapter presents definition and basic characteristics of cloud computing. The second part consists of PESTL analysis that describes the impact of macro-environmental factors (namely political, economical, social, technological and legal factors) on the use of cloud computing in public sector institutions. The third part presents SWOT analysis of cloud computing and its use in public sector. The fourth chapter presents a case study of the implementation of cloud computing services at The Faculty of Arts of the Charles University.

The results of the conducted analysis tend to positive effects of cloud computing use in public sector institutions, presuming a proper risk analysis is done before implementation begins.

Klíčová slova (anglicky):

Cloud computing, IaaS, PaaS, SaaS, public sector, PESTL, SWOT, virtualisation

Seznam zkratek

CSA ... Cloud Security Alliance (agentura zabývající se bezpečností cloudových služeb)

ECP ... European Cloud Partnership (Evropské partnerství pro cloud computing)

FCCS ... Federální cloud computingové strategie USA

FedRAMP ... Federal Risk and Authorization Management Program (Federálni program managementu rizik a autorizace)

GAO americký Vládní úřad odpovědnost (Government Accountability Office)

IaaS ... Infrastruktura jako služba

ICT ... informační a komunikační technologie

PaaS ... Platforma jako služba

PESTL ... analytická technika (akronym pro politické, ekonomické, sociální, technologické a legislativní okruhy)

RVIS ... Rada vlády pro informační společnost

SaaS ... Software jako služba

SLA ... smlouva o úrovni poskytovaných služeb (Service level agreement)

SOA ... servisně orientovaná architektura

SWOT ... analytická technika (Strenghts - silné stránky, Weakness - slabé stránky, Opportunities - příležitosti, Threats - hrozby)

UPCCE .. Uvolňování potenciálu cloud computingu v EU (strategie EU)

VM ... virtuální stroj (virtual machine)

Obsah

Předmluva

Tématem této diplomové práce je analýza přínosů a rizik spojených s využitím cloud computingu, tedy poskytování informačních a komunikačních technologií v podobě služby dodávané přes Internet, v institucích veřejného sektoru.

V současné době se jedná o velmi aktuální téma, jehož zpracování z pohledu veřejného sektoru zatím nebylo podrobně provedeno a jedná se o první kvalifikační práci zabývající se cloud computingem na Ústavu informačních studií a knihovnictví.

Diplomová práce je rozdělena do čtyř hlavních kapitol. První kapitola se věnuje samotné technologii označované jako cloud computing. Součástí této kapitoly její definice, popis základních vlastností a stručný úvod do historie vývoje této technologie. Prostor je dále věnován technologickým základům cloud computingu a úvodní část je ukončena popisem životního cyklu cloud computingu.

Druhá a třetí kapitola přináší vlastní analýzu přínosů a rizik využití cloud computingu v institucích veřejného sektoru. Analýza je zaměřena na služby cloud computingu, poskytované v tzv. veřejném modelu, tedy nabízené širokému okruhu potenciálních zákazníků (včetně institucí veřejného sektoru). Pro analýzu byly použity metody PESTL a SWOT, jejichž výstupy jsou shrnuty v závěru práce.

Druhá kapitola (první část analýzy) představuje tzv. PESTL analýzu věnující se vlivu makrookolí na potenciální využití cloud computingu v institucích veřejného sektoru. Analýzou jsou pokryty vlivy politické, ekonomické, sociální, technologické a legislativní.

V rámci třetí kapitoly byla provedena analýza SWOT zaměřená na silné a slabé stránky využití cloud computingu v institucích veřejného sektoru, které vychází z vlastností samotné technologie. Analýza dále rozebírá příležitosti a hrozby plynoucí z tohoto využití a také z vlivu makrookolí, jež bylo zanalyzováno v předchozí kapitole.

K analytickým metodám PESTL a SWOT jsem se uchýlil, neboť byly součástí teoretických i praktických příprav po dobu mého studia na Ústavu informačních studií a knihovnictví, a tak jsem je chtěl uplatnit ve větším měřítku.

Čtvrtá a poslední kapitola obsahuje případovou studii využití konkrétní cloud computingové služby ”Office 365” na Filosofické fakultě Univerzity Karlovy v Praze. Tato kapitola m8 za cíl ilustrovat reálné využití cloudové služby.

Původní záměr práce bylo analyzovat využití cloud computingu v knihovnách, informačních institucích a veřejné správě, jak také vypovídá samotný název práce. V průběhu přípravy a samotné tvorby práce však vyšlo najevo, že takto specifikovaný výběr představuje zbytečné omezení a záběr byl rozšířen na celý veřejný sektor, čímž jsou pokryty i původně specifikované instituce. V tomto ohledu je tedy přesnější oficiální název práce v anglickém jazyce.

Hlavním cílem práce je tedy analyzovat přínosy a rizika spojená s využitím cloud computingu ve veřejném sektoru a to v rámci jednotlivých institucí. Odpovědět by měla také na to, jaký vliv má politická situace, které makroekonomické faktory mohou mít vliv při rozhodování o využíti cloudových služeb, jaký vliv má sociální okruh na využití cloud computingu ve veřejném sektoru, jaká je technologická připravenost poskytovatelů a samotných služeb, jaké legislativní a právní faktory hrají roli při využití služeb veřejného cloudu v institucích veřejného sektoru. A také přinést hodnocení, zda jsou cloudové služby vhodné pro využívání veřejným sektorem.

Práce je tak určena zejména pro veřejné instituce, které přemýšlí o inovaci svých informačních a komunikačních technologií, resp. jejich zástupců na úrovni managementu či jiných pracovníků odpovědných za informační technologie. Případně pro jakékoliv další zájemce o téma cloud computingu či informačních technologií obecně.

Na závěr bych také rád vyjádřil poděkování vedoucí mé práce, PhDr. Heleně Lipkové, Ph.D za konzultace, připomínky a důležitou zpětnou vazbu.

1. Úvodní část

1.1. Definice cloud computingu

Od roku 2006, kdy Eric Schmidt, jeden ze zakladatelů společnosti Google, představil termín cloud computing1 široké veřejnosti [SCHMIDT, 2006], se objevily desítky různých definic cloud computingu. Ani nyní o několik let později stále neexistuje jediná zcela přijímaná definice. To je dáno několika důvody. Za prvé tím, že cloud computing je stále se vyvíjející paradigma a pro různé zájmové skupiny může znamenat něco jiného. Jinak na cloud computing pohlížejí poskytovatelé cloudové infrastruktury a služeb, kteří na cloud pohlížejí více „zevnitř" a jinak samotní uživatelé. Dalším z důvodů je ne úplně sjednocená terminologie, což je způsobeno také velkým počtem komerčních firem, které se cloud computing, tento dnes značně populární termín, snaží „naroubovat" na své služby. A nakonec tím, že cloud computing pokrývá velice široké spektrum technologií a služeb. Jak upozorňuje studie Kalifornské univerzity v Berkeley, cloud computing označuje jak aplikace poskytované v podobě služby, tak i hardware a systémový software v datových centrech, na kterých tyto služby běží. [AMBRUST, 2009]

Další studie [VAQUERO, 2009], která sestavila definici cloud computingu na základě porovnání více než 20 definicí, označuje cloud computing za "velké sdružení jednoduše použitelných a přístupných virtualizovaných zdrojů (jako hardware, vývojářské platformy a/nebo služby). Tyto zdroje mohou být dynamicky konfigurovány tak, aby se přizpůsobily proměnlivé zátěži a zároveň dostupné zdroje optimálně využily. Poplatky za využívání těchto zdrojů jsou obvykle vyučtovány na základě skutečného využití (tzv pay-per-use model VIZ KAP), jež je garantováno poskytovatelem infrastruktury na základě smluvní dohody o úrovni služeb (tzv. SLA, service-level agreement)"

V současnosti patrně nejrozšířenější a všeobecně nejakceptovatelnější definici cloud computingu vytvořil americký Národní institut standardů a technologie (NIST, National Institute of Standards and Technology). Dle této definice je cloud computing „model umožňující všudypřítomný a pohodlný síťový přístup ke sdílenému seskupení konfigurovatelných výpočetních zdrojů (např. sítí, serverů, úložišť, aplikací a služeb) dle

[1] Ohledně původu samotného termínu Cloud computing se stále vedou spory, jeho autorství nebylo dosud nikomu jednoznačně přisouzeno. Za autory bývaji často označování inženýři společnosti Google, případně profesor Ramnath Chellapa, který termín Cloud computing použil jako první na akademické půdě.

potřeby, který může být rychle a jednoduše realizován, a to i s minimální interakcí s poskytovatelem služby."

Definice NIST dále popisuje pět základních charakteristik (samoobslužná služba na vyžádání, široký síťový přístup, sdílení prostředků, vysoká pružnost, měřitelná služba), tři servisní modely (IaaS, infrastruktura jako služba; PaaS, platforma jako služba; SaaS, software jako služba) a čtyři modely nasazení cloudu (privátní, veřejný, hybridní a komunitní), které definici dále rozvíjejí a vysvětlují (viz následující kapitoly).

1.2. Historie konceptu cloud computingu

Cloud computing se neobjevil náhle, jako nějaký revoluční vynález, ale spíše šlo o přirozený vývoj výpočetních technologií, který byl hnán dopředu ekonomickými důvody, tedy snahou o co nejefektnivější využití dostupných prostředků. Koncept podobný cloud computingu měly již sálové počítače (mainframe computers), které začaly být dostupné pro firmy i akademickou sféru v 50. letech 20. století. Pořizovací cena a provozní náklady těchto počítačů byly značně vysoké. Organizace si mohla obvykle dovolit jediný počítač, který byl využíván pro více uživatelů (případně i více organizací). Vzhledem k vysokým nákladům muselo být jejích využití efektivní. To bylo umožněno pomocí tzv. „sdílení času" (time-sharing), kdy jeden počítač byl používán více uživateli najednou skrze jednoduché terminály, jež samy o sobě neměly žadnou výpočetní funkci, ale sloužily k pouhému zadávání dat a jejich zobrazování. Od 2. poloviny 60. let 20. století fungoval již poměrně velký trh s komerčním poskytováním time-sharingu pro malé i středně velké podniky, vědeckou obec a akademické instituce [Anon., 1972]. Jedním z autorů tohoto konceptu byl John McCarthey, který již v roce 1961 předpověděl, že „… výpočetní technologie mohou jednoho dne být organizovány jako veřejná služba, stejně jako jsou veřejnou službou telefonní sítě… počítačové služby by se mohly stát základem nového a důležitého průmyslu" [SCHOFIELD, 2011]. Způsob poskytování výpočetních zdrojů jako veřejné služby se označuje "Utility computing"(viz kapitola). Technologický model, který právě tuto formu poskytování výpočetních služeb umožňuje, je cloud computing.

Dalším důležitým krokem směrem ke cloud computingu byl vznik tzv. virtuálních strojů (Virtual Machines, VM) společnosti IBM v 70. letech 20. století, na kterých mohlo současně fungovat jeden či více operačních systémů. Princip virtualizace se stal katalyzátorem dalšího vývoje informačních technologií a je také hojně využíván pro provoz cloudových služeb (viz kapitola) [NETO, 2014].

V období od 60. let do konce 20. století probíhaly další důležité změny. V 60. letech začal vývoj sítě ARPANET, která se v 90. letech postupně proměnila v celosvětovou síť Internet, která v té době začala být přístupná široké veřejnosti. V 80. letech došlo k rozmachu osobních počítačů, které začínaly být stále více dostupné i pro domácnosti.

V roce 1999 se objevila první služba, kterou lze zpětně označit za „cloudovou". Tou je webová služba Salesforce.com, která je označována za pionýra v poskytování podnikových aplikací (především CRM2) ve formě služby dodávané přes Internet.

V roce 2002 Amazon.com spustil první verzi služby Amazon Web Services, jež zdarma poskytovala webovým vývojářům platformu pro tvorbu nástrojů a aplikací, které si vývojáři mohli implementovat do svých vlastních webových stránek. O čtyři roky později Amazon.com spustil komerční webovou službu Elastic Compute Cloud (označovaný zkratkou EC2), pronajímající zákazníkům virtuální výpočetní zdroje, na kterých mohli provozovat vlastní aplikace a služby. EC2 byla první široce dostupná cloud computingová infrastruktura [ARIF, 2009]. K jejímu vzniku vedlo to, že Amazon.com, původně internetový prodejce knih, měl servery poskytující obří výpočetní kapacitu, které však mimo prodejní špičku zahálely, což bylo značně neekonomické, a tak došlo k nabídnutí vlastních výpočetních zdrojů externím zákazníkům [BROOKS, 2010].

Vznik cloud computingu by nebyl možný bez rozvoje některých technologií. Zejména se jedná o pokrok v oblasti hardwaru (např. multi-jádrové procesory) a možnosti jeho virtualizace, internetových technologií (servisně orientovaná architektura, web 2.0), distribuovaných výpočetních systémů (klastery a gridy) a správě systémů (automatizace datových center). Tyto technologie, na kterých je cloud computing založen, si stručně představíme v následující kapitole.

1.3. Technologické základy cloud computingu

1.3.1. Grid computing

Grid computing, označován za přímého předchůdce cloud computingu [FOSTER, 2008], se objevil v polovině 90. let. Hlavním úkolem bylo řešení složitých vědeckých problémů jako hledání nových léků, ke kterým by jinak byly potřeba velice výkonné a také velice drahé super-počítače [E-SCIENCETALK, 2003a].

Grid[3] computing je technologie sdružování distribuovaných výpočetních zdrojů do jedné společné sítě (ať už počítačů, mobilních telefonů či specifických zařízení jako meteorologické

[2] Customer Relationship Management - aplikace pro správu a řízení vztahů se zákazníky

senzory [STRICKLAND, 2008]), která slouží k řešení jednoho úkolu [HASHEMI, 2012]. Gridová infrastruktura je obvykle vlastněna a využívána více uživateli (organizacemi), kteří mají stejný přístup ke společným zdrojům.

Základními principy gridů jsou sdružování zdrojů (nezávisle na jejich lokaci a použité platformě), dostupných všem uživatelům; důvěra mezi uživateli (podpořená bezpečnostními prvky autentizace a autorizace); efektivní využívání zdrojů založené na využití specializovaného softwaru pro přidělování úkolů; nezávislost na lokaci zdrojů; a využívaní otevřených standardů [E-SCIENCETALK, 2003b].

Principy grid computingu a cloud computing jsou na první pohled velice podobné, ale cloud computing řeší mnohé problémy gridových systémů. Gridové systémy měly značné problémy se spolehlivostí a kvalitou poskytovaných služeb. Jednotlivé zdroje (tzv. uzly) v rámci gridové sítě jsou úzce propojené a selhání jediného uzlu může vést k selhání celého systému. S rostoucí popularitou gridů se začaly objevovat problémy s dostupností zdrojů a někdy též ne zcela férovým chováním uživatelů, na nichž spolehlivost celého gridového systému také stojí. Gridové systémy jsou také více uzavřené vůči externím aplikacím a nenabízejí tak širokou možnost využití jako cloud computing. Cloud computing překonává[4] gridové sítě využitím principů servisně orientované architektury a virtualizačních technik.

1.3.2. Utility computing

Utility computing je označení pro obchodní model poskytování výpočetních zdrojů na vyžádání. Zdroje jsou vlastněny a spravovány poskytovatelem služeb, který je poskytuje uživatelům a dále zpoplatňuje na základě skutečného využití daných služeb (tzv. pay-per-use model)[RAPPA, 2004]. Model utility computingu se snaží o co nejefektivnější využití dostupných prostředků a zároveň o minimalizování nákladů.

Na první pohled by se tedy utility computing dalo lehce zaměnit za cloud computing (a někdy se tak děje), ale ve skutečnosti je cloud computing pouze jeden ze způsobů, jak poskytovat výpočetní zdroje ve formě služby, podobně jako například elektrický proud a vodu.

Cloud comptuing využívá koncepty utility computingu pro měření využítých služeb a následného placení za jejich užití.

---

[3] grid = síť, tedy výpočetní síť (soustava)

[4] To ovšem neznamená, že grid computing by byl úplně překonanou technologií. Stále se velice hodí pro řešení jednotlivých z hlediska výpočetní kapacity velice náročných úkolů.

1.3.3. Autonomic computing

Hlavním cílem autonomních výpočetních systémů je vytvoření takového počítačového prostředí, které je schopno řídit samo sebe s minimálním nebo žádným lidským zásahem. Autonomní výpočetní systémy se dokáží vyrovnat s náhlými změnami, které mohou být způsobeny například nějakou chybou. K tomu slouží sensory, které změnu odhalí, reakční mechanismy, jež na ní zareagují a řídicí systém, který patřičně zhodnotí provedenou reakci [HAMDAQA, 2012].

Velká datacentra poskytovatelů cloudových služeb musí být řízena co nejefektivněji. K vytvoření cloudových infrastruktur a platforem bývají využity právě koncepty autonomních počitačových systémů, jež mají zajistit správu úrovně služeb běžících aplikací, správu kapacity datacenter, obnovu po havárii a automatizaci vytváření virtuálních strojů (více info dále v textu).

1.3.4. SOA a Webové služby

Servisně orientovaná architektura (SOA) je metoda skládání jednotlivých komponent (služeb), tak aby celkový výsledek poskytoval samostatnou službu (která sama je poskládána z jednotlivě fungujících částí). Jednotlivé části jsou samy o sobě plně hodnotnými službami, které mohou být využity samostatně nebo v rámci jiných celků. Orientace na služby je jedním z hlavních paradigmat současného vývoje webových služeb. SOA poskytuje rámec pro vývoj aplikací v tomto duchu [HAMDAQA, 2012].

Obecným příkladem spojení služeb v jeden celek pomocí SOA může být např. nákup zboží po internetu, kdy jedna služba vyhledá požadované zboží, druhá ověří jeho dostupnost, třetí služba vypočítá, po objednání a zadání doručovacích údajů, celkovou cenu, a pro zaplacení je využito dalších navazujících služeb. To je možné díky jednotlivým webovým službám.

Webové služby jsou softwarové systémy vytvořené tak, aby podporovaly vzájemnou síťovou komunikaci mezi aplikacemi [HUGO, 2004]. Díky používaní standardizovaných protokolů pro komunikaci (jako SOAP[5]) postavených na HTTP a XML technologiích, tak dokáží spojit aplikace provozované na odlišných platformách.

Zdroje v rámci cloud computingu, jak již bylo vysvětleno, jsou poskytovány ve formě služby. K tomu, aby tyto služby byly jednoduše dostupné, cloud computing využívá právě standardy a osvědčené postupy servisně orientované architektury.

[5] Simple Object Access Protocol

1.3.5. Virtualizace

Virtualizace je hlavní technologií, která umožňuje provoz cloudových služeb [HAMDAQA, 2012].

Ty jsou obvykle provozovány v obrovských data centrech budovaných pro provoz mnoha různorodých aplikací určených pro velké množství uživatelů. Vhodným prostředkem pro provoz těchto center je právě virtualizace. Virtualizace je tedy hlavní technologií, která je využívána pro provoz cloudové infrastruktury (IaaS).

Virtualizace umožňuje vytvoření několika rozmanitých virtuálních počítačů, které mohou být v jeden okamžik provozovány buď na jediném fyzickém serveru, nebo jejich kolekci. Virtualizovat lze celý počítač (tzv. „virtuální stroj"), nebo samotné hardwarové komponenty jako procesory, datová úložiště, síťové prvky či celé virtuální sítě, ale i softwarové aplikace jako operační systémy (na kterých mohou být instalovány další aplikace). Virtuální stroje lze konfigurovat a jednoduše spustit pomocí souborů označovaných jako obrazy virtuálních strojů (virtual machine images, VMI). Pro pohodlnost uživatelů jsou poskytovateli služeb často nabízeny již předkonfigurované soubory VMI. Spustit virtualizovaný server je tedy možné během několika minut [HON, 2013].

Jediný fyzický server, či jejich kolekce, může hostit nezávislé virtuální stroje pro odlišné uživatele. Ti jsou odděleni pouze softwarovou vrstvou, která má na starosti řízení a přístup virtuálních strojů k fyzickému serveru, označovanou jako hypervizor. Hypervizor poskytuje virtuální hardwarové prostředky hostovaným operačním systémům a umožňuje, aby velké množství fyzických serverů (a k nim připojené síťové prvky a úložiště dat) mohlo fungovat jako jeden celek.

Hlavními cíli virtualizace tedy jsou: plné využití sdílených prostředků pomocí dynamické alokace zdrojů; centralizace řízení zdrojů; zvýšení pružnosti a škálovatelnosti datových center; poskytnout izolaci potřebnou pro bezpečnost a soukromí; vytvořit základ pro samoobslužné prostředí. Vlastnosti „sdílení prostředků" a "vysoká pružnost" cloudových služeb jsou možné právě díky virtualizačním technikám.

1.4. Základní vlastnosti cloudových služeb

1.4.1. Samoobslužná služba na vyžádání (On-demand self-service)

Uživatel si může automaticky obstarat výpočetní zdroje dle vlastní potřeby a bez nutnosti lidské interakce s poskytovatelem služby [MELL, 2011].

Objednání služby je obvykle možné online přes webové rozhraní samoobslužného portálu, který nabízí katalog služeb. Uživatel si může například vybrat počet a typ virtuálních strojů, velikost úložných prostor (v rámci IaaS), operační systém (v rámci PaaS) atd. Takto lze využít předpřipravené služby, zprovoznění nestandardních požadavků může trvat déle [LEŠTINA, 2011].

1.4.2. Široký síťový přístup (Broad network access)

Výpočetní zdroje jsou dostupné přes síť a zpřístupněny skrze standardní mechanismy, které podporují využití tenkých i tlustých heterogenních klientských platform (jako jsou různé webové prohlížeče, mobilní telefony, tablety, laptopy či terminály) [MELL, 2011].

Cloudové služby podporují nejen přístup z mnoha rozličných koncových zařízení, ale také prakticky z jakéhokoliv místa (alespoň pokud se lze připojit k Internetu). Aby služba byla dostupná pomocí různých zařízení, je nutné důsledné využívání standardizovaných rozhraní a přístupových mechanismů.

Široký síťový přístup je výhodný jak pro uživatele, kteří mohou služby využívat nezávisle na druhu svého zařízení, tak pro poskytovatele služeb, kterým se tak rozšiřuje potenciální zákaznická báze.

1.4.3. Sdílení prostředků (Resource pooling)

Výpočetní zdroje poskytovatele služeb jsou sdružovány tak, aby mohly sloužit více zákazníkům najednou. Fyzické i virtuální zdroje jsou dynamicky přerozdělovány dle potřeby uživatelů. Uživatel obvykle nemá žádnou znalost ani kontrolu nad tím, kde přesně se výpočetní zdroje nacházejí. V některých případech může být dovoleno specifikovat umístění zdrojů na vyšším abstraktním stupni (např. zemi umístění zdrojů) [MELL, 2011].

Dynamické přerozdělování sdílených prostředků na základě skutečné potřeby pro využití zdrojů umožňuje poskytovatelům udržet maximální úroveň služeb s minimálním počtem zdrojů, což zároveň snižuje cenu služeb pro uživatele, nikoli však jejich kvalitu.

Výpočetní zdroje mohou být sdíleny na úrovni všech tří servisních modelů (infrastruktura, platforma, software - VIZ KAP). Typicky se to děje pomocí virtualizačních technik (VIZ KAP), a to na nejnižší (infrastrukturní) vrstvě. Virtualizace vyšších vrstev je méně obvyklá, jednotlivé instalace na úrovní platformy a softwarových aplikací jsou obvykle odděleny již na základní vrstvě. Některé aplikace však mohou sdílet i stejnou infrastrukturu (od hardwaru po operační systém) a zároveň sloužit více uživatelům, kteří jsou však odděleni a nesdílí a nevidí svá data [GARTNER, 2013].

1.4.4. Vysoká pružnost (Rapid elasticity)

Výpočetní zdroje mohou být poskytovány pružně, v některých případech i automaticky, a to úměrně dle potřeby klienta. Zdrojů by tedy mělo být poskytováno právě tolik, kolik jich je potřeba. Z pohledu uživatele to často vypadá, jako by zdroje byly dosažitelné v jakémkoliv množství a v jakýkoliv okamžik [MELL, 2011].

Vysoká pružnost bývá často zaměňována za škálovatelnost (scalability), jež je ale předpokladem pro vysokou pružnost cloudových služeb. Škálovatelnost je schopností systému zvládnout zvyšující se zátěž využitím dodatečných zdrojů [HERBST, 2013].

1.4.5. Měřitelná služba (Measured service)

Cloudové systémy automaticky kontrolují a optimalizují zdroje za použití měřících kapacit na daném stupni abstrakce, která je závislá na využité službě (např. úložiště dat, zpracování dat, šířka pásma či aktivní uživatelské účty). Využití zdrojů může být monitorováno, kontrolováno a reportováno, čímž je zajištěna transparentnost pro poskytovatele i uživatele dané služby [MELL, 2011].

Tato vlastnost je nezbytná, zvlášť pokud jsou uživatelům služby účtovány na základě jejich využívání. Různé modely zpoplatnění cloudových služeb jsou popsány v ekonomickém okruhu PESTL analýzy.

1.5. Modely nasazení

Model nasazení cloudu poskytuje základní charakteristiku způsobu správy a umístění výpočetních zdrojů. Model cloud computingu dle NIST popisuje čtyři základní modely nasazení: privátní, veřejný, komunitní a hybridní. S tím, že poslední dva jsou různými kombinacemi privátního a veřejného modelu.

1.5.1. Privátní cloud (Private cloud)

Cloudová infrastruktura je poskytována výhradně pro účely jediného uživatele. Vlastníkem infrastruktury může být jak samotný uživatel, tak i třetí strana (případně kombinace obou) [MELL, 2011].

Umístění cloudové infrastruktury může být v prostorách patřících uživateli (tzv. on-premise) nebo mimo ně (tzv. off-premise). Druhý případ nastává, když provozovatel nějakého veřejného cloud vyhradí část své infrastruktury pro výhradní užívání jediného zákazníka. Takové řešení se označuje jako virtuální privátní cloud [GHOSH, 2011].

Privátní cloud poskytuje uživatelům prakticky veškeré výhody cloudových služeb. Uživatel není limitován kvalitou internetového spojení, a také není vystaven bezpečnostním rizikům (podrobně rozebrány ve SWOT analýze) a právním problémům (více viz příslušná kapitola PESTL analýzy), které s sebou může přinášet využívání veřejného cloudu[6].

Nevýhodami tohoto řešení jsou ovšem velké pořizovací náklady a náročná správa - obzvlášť pokud se uživatel rozhodne pro stavbu vlastní infrastruktury. Pořízení vlastní (privátní) cloudové infrastruktury má smysl především pro velké organizace, které dokáží lépe těžit z výhod velkého počtu sdílených prostředků [HARDING, 2011].

Příkladem virtuálního privátního cloudu může být služba „Amazon Virtual Private Cloud" provozována firmou Amazon. K používání privátních cloudů v ČR se zatím hlásí především velké organizace jako ČEZ, T-Mobile či Raiffeisenbank [VOLF, 2012].

1.5.2. Veřejný cloud (Public cloud)

Infrastruktura cloudu je poskytována pro využití širokou veřejností. Může být vlastněna, provozována a spravována soukromou firmou, akademickou nebo státní organizací, případně jejich kombinací. Infrastruktura by se měla nacházet v prostorech poskytovatele služeb [MELL, 2011].

Služby poskytovatelů veřejného cloudu mohou být zpoplatněny nebo poskytovány zdarma. Infrastruktura je obvykle využívána více zákazníky poskytovatele, čímž dochází k jejímu efektivnějšímu využití. Z tohoto důvodu bývá toto řešení z finančního hlediska nejvýhodnější. Také odpadá starost o správu infrastruktury a zprovoznění služeb na veřejném cloudu je velice rychlé.

Veřejné cloudy provozují prakticky všichni velcí poskytovatelé cloudových služeb jako Amazon, Google, Microsoft a další. V České republice za zmínku stojí veřejný cloud Českých radiokomunikací.

1.5.3. Komunitní cloud (Community cloud)

Infrastruktura cloudu je poskytována pro výhradní využití specifickou komunitou uživatelů z organizací sdílejících stejné zájmy. Infrastruktura může být vlastněna, provozována a spravována jednou či více organizacemi v rámci komunity, třetí stranou nebo jejich kombinací. Infrastruktura se může nacházet v prostorách poskytovatele i mimo ně [MELL, 2011].

[6] Některé, obzvlášť právní, problémy musí být však brány v potaz v případě, kdy uživatel využívá dedikované infrastruktury provozovatele, který tak může mít dále přístup k datům uživatele.

Pokud se na výstavbě komunitního cloudu podílí více uživatelů, pak mohou být finanční nároky podstatně menší než v případě výstavby privátního cloudu a přesto si takové řešení ponechá právě jeho výhody.

Komunita může představovat organizace ze stejného odvětví jako např. zdravotnictví, bankovnictví, případně vládní organizace.

1.5.4. Hybridní cloud (Hybrid cloud)

Cloudová infrastruktura je složena z alespoň dvou druhů infrastruktur (privátní, komunitní nebo veřejná), které jsou stále jedinečnými entitami, ale jsou propojeny pomocí standardizovaných, případně proprietárních, technologií, jež umožňují přenositelnost dat a aplikací [MELL, 2011].

Nabízí se několik scénářů, jak může být hybridní cloud spravován. Jedním z nich je, že organizace využívá služeb veřejného cloudu pro některé své aplikace nebo zálohu dat, ale kriticky důležité aplikace a privátní data si ponechává ve svém privátním cloudu [ROUSE, 2013].

Hybridní cloudové prostředí může být také spravováno zprostředkovatelem cloudových služeb, který kumuluje funkce několika cloudových služeb a buduje na nich službu s přidanou hodnotou.

1.6. Servisní modely

Cloud computing je především o poskytování služeb a to od základní výpočetní kapacity po značně sofistikované softwarové aplikace. Servisní modely poskytují (hrubé) rozlišení toho, co je v rámci cloudových služeb nabízeno. Kromě zde popsaných servisních modelů dle NIST se lze setkat ještě s dalšími modely, kterými jsou například bezpečnost jako služba či identita jako služba.

1.6.1. Infrastruktura jako služba (IaaS, Infrastructure as a Service)

V rámci modelu IaaS jsou uživateli poskytovány základní výpočetní zdroje pro zpracování dat, datová úložiště, sítě a další zdroje. Na poskytnutou infrastrukturu si může uživatel instalovat libovolný software, od operačního systému po aplikace sloužící konečným uživatelům. O fyzickou vrstvu infrastruktury se nestará uživatel, ale právě poskytovatel cloudu. Abstraktní, tedy softwarová vrstva je již plně v rukou uživatele [MELL, 2011].

I když zprovoznění této služby bývá řešeno skrze uživatelsky příjemná prostředí a může být otázkou několika minut, je k tomu třeba zkušených IT pracovníků. Uživatel může mít limitovanou kontrolu nad výběrem použitých komponentů.

Příklady: Amazon EC2, Google Compute Engine, Microsoft Azure

1.6.2. Platforma jako služba (PaaS, Platform as a Service)

Prostředky poskytované uživateli v prostředí PaaS jsou určeny pro podporu vlastního vývoje a údržby aplikací dostupných přes Internet. Vývoj a správa aplikací je možná pouze za využití prostředků (jako programovací jazyky, knihovny a další nástroje) podporovaných poskytovatelem cloudu. Uživatel nespravuje ani nemá kontrolu nad spodní vrstvou infrastruktury (sítě, servery, operační systém ani datová úložiště), ale kontroluje vše nad ní [MELL, 2011].

Příklady: Microsoft Azure, Google App Engine, IBM Bluemix

1.6.3. Software jako služba (SaaS, Software as a Service)

V případě modelu SaaS mají prostředky poskytované uživateli podobu využívaní aplikací provozovaných na cloudové infrastruktuře poskytovatele. Aplikace jsou dostupné prostřednictvím rozhraní rozličných tenkých klientů, jako je např. webový prohlížeč, nebo rozhraní samotného programu. Uživatel nespravuje ani neřídí cloudovou infrastrukturu, na které je aplikace provozována. Uživateli může být povoleno spravování některých specificky uživatelských nastavení [MELL, 2011].

Nejznámějšími představiteli SaaS jsou patrně online kancelářské balíky od Microsoftu (Office 365), Googlu (Google Docs) a sociální sítě (jako Facebook či Twitter). Nejstaršími SaaS aplikacemi jsou nejspíše online e-mailové služby, které také spadají pod definici SaaS. Tím výčet SaaS zdaleka nekončí. Dnes prakticky všechny desktopové aplikace získávají svoji online verzi spadající pod kategorii SaaS.

1.7. Základní role v cloudu

Pro přehlednost je třeba definovat také základní role, které mohou zastávat jednotliví účastníci v rámci poskytování a využívaní cloudových služeb. Referenční model NIST definuje 5 základních rolí: uživatel, poskytovatel, auditor, zprostředkovatel a nosič [LIU, 2011]. Každá role je zastávána subjektem, jímž může být právnická i fyzická osoba a jeden subjekt může zároveň zastávat i více rolí najednou.

Uživatel cloudu (Cloud Consumer): Subjekt využívající jednu nebo více cloudových služeb poskytovatele, se kterým vstupuje do právního vztahu. Dle způsobu využití cloudových

služeb může uživatel vstupovat do dalších rolí - např. do role poskytovatele, pokud využívá prostředí PaaS pro vybudování nové služby, kterou dále poskytuje.

V rámci této diplomové práce je za uživatele považována instituce veřejného sektoru pokud není zdůrazněno jinak (např. že se jedná o koncového uživatele - v tomto případě se jedná o nespecifikovanou fyzickou osobu).

Poskytovatel cloudu (Cloud Provider): Subjekt zodpovědný za tvorbu a zpřístupnění cloudové služby uživateli. Poskytovatel je zodpovědný za tvorbu služby, správu infrastruktury potřebné pro provoz služby, poskytování služby dle dohody o úrovni poskytovaných služeb a v neposlední řadě zajišťuje bezpečnost služby [LIU, 2011].

Zprostředkovatel cloudu (Cloud Broker): Zprostředkovatel je 3. strana vstupující do vztahu mezi poskytovatelem cloudu a koncovým uživatelem. Základními činnosti zprostředkovatele jsou samotné **zprostředkování** (často s přidanou hodnotou ke službě), **agregace** (spojení jednotlivých cloudových služeb i od více poskytovatelů do jedné) a **přizpůsobení** služeb pro uživatele [VOJKOVSKÝ, 2013].

Auditor cloudu (Cloud Auditor): Subjekt, který může provádět nezávislý audit cloudových služeb a to zejména v oblasti řízení rizik (např. bezpečnost privátních dat) a celkového dodržování dohodnuté úrovně poskytovaných služeb.

Nosič (Cloud Courrier): Prostředník, který poskytuje a stará se o spojení mezi poskytovatelem a uživatelem cloudových služeb [LIU, 2011].

1.8. Životní cyklus využití cloudových služeb

V rámci této kapitoly se zaměříme na životní cyklus využití služeb veřejného cloudu (tak jak je definován VIZ KAP), a to z pohledu jeho využití institucí veřejného sektoru (uživatel). Rozebereme tedy jednotlivé kroky, kterými musí instituce projít při rozhodování o využití cloudových služeb a jejich případnému nasazení.

Na rozdíl od Spojených států a dalších zemí, které zavedly politiku „cloud-first" (VIZ KAP), nejsou veřejné instituce v ČR nijak povinny cloudové služby využívat a ani jejich nasazení zvažovat. Následující rozbor životního cyklu cloudových služeb předpokládá alespoň zájem o aktualizaci, inovaci či rozšíření současného IT portfolia veřejné instituce.

Životní cyklus využití cloudových služeb se dá rozložit na čtyři základní fáze:

1. Iniciační fáze.

2. Akvizice cloudových služeb.

3. Provoz cloudových služeb.

4. Ukončení provozu cloudových služeb.

1.8.1. Iniciační fáze

Samotnou iniciační fázi lze rozdělit na několik kroků, kterými by měl uživatel projít při zvažování využití cloudových služeb.

Prvním takovým krokem je ohodnocení vlastních ICT zdrojů. V rámci tohoto hodnocení je třeba zvážit, v jaké fázi svého životního cyklu se nacházejí ICT zdroje instituce. Pokud jsou na konci svého životního cyklu nebo se k němu blíží (např. dosluhující servery či blížící se vypršení platnosti licencí na softwarové aplikace), pak je třeba rozhodnout další postup. A cloudové služby by mohly být vhodnou alternativou.

Druhým krokem je samotné seznámení se s cloud computingem, jeho vlastnostmi a službami, které nabízí. V rámci této práce se v tomto pořadí těmto tématům věnují především tyto kapitoly: VIZ KAP

Na základě výše zmíněných kroků je třeba zvážit, které IT zdroje lze přesunout do cloudového prostředí, protože ne všechny ICT zdroje jsou pro přesun vhodné. Případně jejich varianta v podobě cloudové služby nemusí existovat. Některými otázkami, na které by se instituce měla zaměřit, jsou: Lze v cloudu nalézt levnější řešení? Zvládají současné zdroje zatížení v provozních špičkách[7]? Vyžadují některé zdroje neustálou údržbu [CLOUD.CIO.GOV., 2014a]?

Dalším krokem by měl být průzkum trhu, jehož cílem je zmapování, zda požadované cloudové řešení existuje.

Posledním krokem této fáze je zhodnotit možné přínosy a rizika využívání cloudové služby či přenesení vybraného zdroje do cloudového prostředí. Je třeba brát v potaz, o jaký servisní model se jedná, způsob, jakým uživatelé (případně jiné aplikace) přistupují ke službám, zhodnotit citlivost dat, která se dostanou do cloudu. Výhody a rizika využití cloudových služeb jsou podrobněji rozebrány ve SWOT analýze.

1.8.2. Akvizice cloudových služeb

Akvizice cloudových služeb klade rozdílné nároky na uživatele oproti klasickému nákupu IT zdrojů, který vede k jejich vlastnictví. V případě využívání cloudových služeb zůstávají zdroje ve vlastnictví poskytovatele. Jeden z hlavních rozdílů se tedy týká nastavení

[7] Na UK bychom se například mohli ptát, zda servery, na kterých běží studijní IS, zvládají zátěž v době zápisů předmětů.

smluvního rámce mezi uživatelem a poskytovatelem. Tomu se podrobně věnuje legislativní okruh PESTL analýzy.

Instituce veřejného sektoru jsou při akvizici cloudových služeb (a nejen jich) vázány zákonem č. 137/2006 Sb., o veřejných zakázkách, a to ve chvíli, kdy předpokládaný finanční objem za požadované služby přesáhne limit 2.000.000 Kč (menší zakázky, označované jako zakázky malého rozsahu, nejsou tímto zákonem vázány). Problematika veřejných zakázek je podrobněji popsána v legislativním okruhu PESTL analýzy.

1.8.3. Provoz cloudových služeb

Před samotným provozem cloudových služeb je třeba vytvořit migrační plán a provést samotnou migraci, která by měla být ošetřena písemnou smlouvu, jež je popsána v (VIZ KAP).

Provoz cloudových služeb by měl být předem naplánován a to zejména s ohledem na integraci s již provozovanými aplikacemi, organizačními procesy, zajištění potřebného internetového připojení, zvládnutí případných incidentů, správu a monitorování cloudových služeb [CLOUD.CIO.GOV., 2014b].

Popis samotného managementu využívání cloudových služeb není cílem této práce, ale rizika, která mohou v průběhu využívání nastat, jsou součástí SWOT analýzy (VIZ KAP)

Průběh provozu cloudových služeb by měl být pravidelně monitorován (k čemuž by cloudové služby ze své definice měly obvykle samy poskytovat nástroje) a vyhodnocován především vůči smluvní dohodě o úrovni poskytované služby (ta je popsána v legislativním okruhu PESTL analýzy).

1.8.4. Ukončení provozu cloudových služeb

K ukončení provozu cloudových služeb může dojít z mnoha důvodů, ať už jde o ukončení smluvního vztahu na základě uplynutí předem stanovené doby a nenavázání dalšího smluvního období, či porušení smluvního vztahu některou ze zúčastněných stran. V každém případě by měla být předem připravená strategie odchodu od poskytovatele (exit strategie), která je blíže popsána legislativním okruhu PESTL analýzy.

2. PESTL Analýza

2.1. Základní informace o PESTL analýze

V rámci této podkapitoly bude představena PESTL analýza, popsána metoda a východiska vzniku zde předkládané PESTL analýzy.

2.1.1. Definice PESTL analýzy

PESTL (akronym pro Politické, Ekonomické, Sociální, Technologické, Legislativní okruhy) analýza je analytická technika pro strategickou analýzu vnějšího prostředí organizace [MANAGEMENTMANIA.COM, 2013a]. Existují i další varianty, jež okruhy přidávají (PESTLE - s přídavkem enviromentálního okruhu) či ubírají (PEST - bez okruhu legislativního). V rámci jednotlivých okruhů jsou analyzovány faktory, které nejvíce ovlivňují danou organizaci či jiný subjekt, pro který je analýza prováděna. Samotné faktory se vždy liší v závislosti na oblasti, ve které daná organizace působí.

Historie vzniku PESTL analýzy není příliš zdokumentována a její původ je nejasný. Některé prameny datují první zmínky o využití této analytické techniky na přelom 60. a 70. let 20. století [DCOSTA, 2012].

2.1.2. Metoda práce

PESTL analýza v této diplomové práci je psána pro potřeby nespecifikované instituce veřejného sektoru se zájmem o využití cloud computingu. Tento předpoklad je hlavním východiskem zpracované analýzy. Původním záměrem bylo vytvořit PEST analýzu, ale při teoretické přípravě vyšlo najevo, že je třeba rozšíření o legislativní oblast, která je z hlediska práce velmi podstatná.

Metoda práce na samotné analýze vypadala následovně. Nejprve byla provedena zmíněná teoretická příprava, která vycházela ze studia odborné literatury (především článků), právních předpisů, strategických vládních dokumentů, analýz předních poradenských společností a příspěvků z odborných konferencí. Dalším krokem byla identifikace hlavních faktorů, které mohou mít vliv na využití cloud computingu ve veřejném sektoru. Následovala syntéza informací z nastudovaných zdrojů a jejich aplikace na identifikované faktory s přidáním autorského hodnocení, jež ukončuje většinu popisů jednotlivých analyzovaných faktorů (resp. podkapitol).

Zdroje zabývající se cloud computingem a jeho možným využitím institucemi veřejného sektoru v ČR jsou značně limitované a to především z hlediska využití služeb veřejného cloudu. V doplnění tohoto informačního nedostatku spočívá hlavní přínos této PESTL analýzy. Ta by měla sloužit jako základní přehled vnějších faktorů, které musí vzít instituce veřejného sektoru v potaz, pokud se chce zabývat využitím služeb veřejného cloudu.

Na PESTL analýzu dále navazuje SWOT analýza, která je představena v následující kapitole, kde je také vysvětlen jejich vzájemný vztah.

2.2. Politický okruh

Politický okruh PESTL analýzy se zabývá vztahem státní politiky vůči využití cloud computingu ve veřejném sektoru a to nejen v rámci ČR. První podkapitola zkoumá přístup EU ke cloud computingu, jež má následně vliv i na prostředí v ČR. Analýza se také podrobněji věnuje Spojeným státům, které jsou průkopníky ve využívání cloud computingu ve veřejném sektoru, a Velké Británii, která nasadila patrně nejúspěšnější strategii pro využití cloud computingu ve veřejném sektoru. Poslední část rozebírá situaci v České republice.

2.2.1. Strategie podpory cloud computingu v Evropské unii

První zmínky o výhodách využívání cloud computingu v rámci Evropské unie zazněly v roce 2009 v projevu Viviane Redingové, tehdejší komisařky pro telekomunikace a média, na Lisabonském koncilu v Bruselu. Viviene Redingová cloud computing označila za jeden z nástrojů, který by mohl pomoci malým a středním podnikům fungovat s větší produktivitou díky přechodu od fixních k variabilním IT nákladům, a tím také pomoci rozhýbat celou evropskou ekonomiku, jež byla v té době zasažena ekonomickou krizí a také za jeden z nástrojů pro přechod na nízkouhlíkové hospodářství. Zároveň také přiznala, že Evropa v přijetí a využívání cloud computingu zaspala za USA [REDING, 2009].

V září roku 2012 byla Evropskou komisí přijata strategie nazvaná „Uvolnění potenciálu cloud computingu v Evropě" [EVROPSKÁ KOMISE, 2012], která má vést k zrychlení adopce a širšímu využití cloud computingu napříč všemi sektory ekonomiky. Evropská komise si od přijetí a hlavně plnění této strategie slibuje vytvoření 2,5 miliónů nových pracovních míst a zvýšení HDP Evropské unie o 160 miliard EUR (tedy přibližně o 1 %) a to vše do roku 2020[8].

[8] Toto jsou průměrné hodnoty. Studie IDC (CATTANEO, 2012) hovoří o podílu cloud computingu 88 miliardami EUR na tvorbě HDP v případě, že nedojde k přijetí politiky podporující cloud computing. V případě, že k podpoře dojde, tak by se cloud computing měl podílet až 250 miliardami EUR na tvorbě HDP.

Tato strategie je součástí „Digitální agendy pro Evropu", což je první ze sedmi stěžejních iniciativ desetileté strategie pro udržitelný růst a rozvoj EU nazvané „Evropa 2020". "*Obecným cílem Digitální agendy je zajistit udržitelný hospodářský a sociální přínos jednotného digitálního trhu založeného na rychlém a superrychlém internetu a interoperabilních aplikacích*."[MV ČR, 2012] Cloud computing je řešen v rámci 6. pilíře Digitální agendy pro Evropu.

Strategie UPCCE zahrnuje 3 hlavní akce, pro jejichž vykonání bylo sestaveno několik pracovních skupin.

- **Radikální řešení nepřehledné situace v oblasti norem.**
- **Zajištění bezpečných a spravedlivých smluvních podmínek.**
- **Vytvoření Evropského partnerství pro cloud computing na podporu inovací a růstu ze strany veřejného sektoru.**

První akce se zabývá jednou z hlavních překážek, která znesnadňuje implementaci cloudových služeb. Tou je existence velkého množství technickým norem, jež mohou být pro uživatele značně nepřehledné. Pro uživatele je také prakticky nemožné ověřit, zda poskytovatelé skutečně technické normy dodržují a zda je tak zaručena např. interoperabilita cloudových služeb. K tomu je třeba vytvoření certifikací (případně uznání již existujících certifikací), které by dodržování norem potvrzovaly (více viz technologická část PEST analýzy).

V rámci této akce byl pověřen Evropský ústav pro telekomunikační normy (ETSI) sestavením seznamu všech dostupných norem relevantních pro cloud computing, který byl publikován v prosinci 2013. Dále Evropská agentura pro bezpečnost sítí a informací (ENISA) sestavila list používaných certifikací, jež budou dále evaluovány[citace].

Druhá akce je zaměřena na vytvoření modelových smluvních podmínek pro využívání cloudových služeb. V současnosti používají poskytovatelé často složité smlouvy nebo dohody o úrovni poskytovaných služeb (SLA), jež bývají předem stanovené a případní uživatelé nemají možnost do nich zasahovat.

Cílem je vytvoření modelových smluvních podmínek, které by regulovaly otázky nepokryté společnou evropskou právní úpravou prodeje. Zejména se jedná o otázky spojené s daty uživatelů cloudových služeb (např. co se stane s daty po skončení smlouvy).

V rámci třetí akce založila Komise EU v roce 2012 Evropské partnerství pro cloud computing (dále ECP, z European Cloud Partnership), jež se skládá ze zástupců veřejného i soukromého sektoru pod vedením estonského prezidenta Toomase Hendrika Ilvese. Hlavním úkolem ECP je pracovat na vytvoření společných požadavků pro lepší zadávání veřejných zakázek na cloudové služby.

Dosavadním výsledkem práce ECP je vytvoření rámce pro definování společných osvědčených postupů při zavádění cloudových služeb do praxe. Tento rámec nese označení „Trusted Cloud Europe".

Součástí ECP je také projekt „Cloud pro Evropu", který se zaměřuje na vytvoření požadavků pro zadávání veřejných zakázek v předobchodní fázi pro veřejný sektor v Evropě.

Součástí strategie UPCCE není budování cloudové infrastruktury vyhrazené pro poskytování cloudových služeb uživatelům z evropského veřejného sektoru (tedy jakéhosi evropského „super-cloudu"). Strategie naopak směřuje k vytvoření legislativního rámce, jehož naplnění by mělo vést k tomu, aby veřejně dostupné nabídky cloudových služeb (tedy tzv. veřejný cloud), splňovaly evropské standardy (ve smyslu konkurenceschopnosti, otevřenosti a bezpečnosti). Zároveň však není cílem vyloučit možnost vytvoření vlastních cloudových infrastruktur institucemi veřejného sektoru, zvláště pokud zpracovávají vysoce citlivá data. Avšak, jak upozorňují autoři strategie [EVROPSKÁ KOMISE, 2012a]: '*... i služby cloud computingu, které používá veřejný sektor, by měly, pokud je to možné, podléhat zásadám hospodářské soutěže na trhu, aby bylo zajištěno co nejlepší zhodnocení vynaložených prostředků, a zároveň by měly být dodrženy regulační povinnosti nebo širší cíle veřejné politiky s ohledem na hlavní provozní kritéria, jako je bezpečnost a ochrana citlivých údajů"*

Postup naplňování strategie UPCCE považuje autor za poněkud pomalý, ačkoliv se zdá, že je z velké části naplňována v rámci stanovených termínů. Také je třeba ocenit, že v rámci jednotlivých pracovních skupin skutečně dochází ke spolupráci odborníků z veřejného sektoru i komerční sféry, jak dokládají jejich personální složení, která jsou veřejně dostupná na patřičných stránkách oficiálního webového portálu EU Europa.eu, kde lze také nalézt záznamy jednání těchto skupin, jež jsou tak velmi transparentní.

Strategie UPCCE je součástí širší strategie pro vytvoření jednotného digitálního trhu, jež by umožnil jednodušší vstup nových digitálních služeb na evropský trh, jež je v současnosti komplikován rozdílnou legislativou všech 28 států EU. Vytvoření jednotného digitálního trhu by tak mohlo zjednodušit nejen využívání cloud computingu napříč všemi sektory.

2.2.2. Cloud computing v USA

Spojené státy byly první zemí, která se rozhodla pro využívání cloud computingu na národní úrovni. V roce 2009 (tedy hned rok poté, co se pojem cloud computing rozšířil) byla zahájena „*Federální cloud computingová inciativa*" (The Federal Cloud Computing Initiative, dále FCCI) pro implementaci cloudových řešení na úrovni federálních institucí[9]. O rok později byl spušťen tzv. „*25 bodový implementační plán reformy federálního IT managementu*", jehož součástí byl přechod federálních úřadů k tzv. „*Cloud-first policy*".

„Cloud-first policy" je v poslední době častěji se objevující termín, protože k této politice se začíná uchylovat stále více zemí. Obecně to znamená, že instituce veřejného sektoru musí v případě nějaké IT akvizice nejprve zvážit nasazení cloudového řešení. V jednotlivých zemích se tato politika samozřejmě liší dle lokální legislativy.

Cloud-first policy se v USA týká všech federálních institucí (a institucí v jednotlivých státech, kde bylo toto opatření přijato na státní úrovni jako např. Kalifornie a Havaj), které jsou povinny implementovat cloudové řešení nahrazující již existující IT prostředky, a to nezávisle na tom v jaké fázi životního cyklu se současné IT řešení nachází. Pokud tedy existuje nějaké bezpečné, spolehlivé a cenově výhodné cloudové řešení. Tato politika je prosazována v rámci „*Federální cloud computingové strategie"* (FCCS), prosazené tehdejším CIO Vivekem Kundrou za podpory prezidenta Obamy. Nasazení této strategie mělo vést ke snížení ročních ICT nákladů z 80 mld. USD na 60 mld. USD [KUNDRA, 2011].

Kolem FCCS vzniklo několik souvisejicích iniciativ. Hlavní z nich je „FedRAMP[10]", což je program sloužící k bezpečnostnímu hodnocení a průběžnému monitorování cloudových služeb. Federální instituce mohou využivat pouze cloudové služby, které byly v rámci tohoto programu schváleny. Jedním z cílů programu FedRAMP je snížení duplicitní práce, dříve si každá agentura musela bezpečnostní hodnocení provádět sama. Seznam schválených služeb je dostupný na oficiálním webu programu FedRAMP. V současnosti se jedná o 13 plně schválených služeb, což není mnoho. Certifikační proces je velice důsledný a díky tomu také

[9] V USA označovány jako agentury (agencies). Patří mezi ně např. i Kongresová knihovna

[10] Federal Risk and Authorization Management Program (Federálni program managementu rizik a autorizace)

zdlouhavý. Například certifikace cloudové služby Googlu pro e-mail trvala celý rok [FIGLIOLA, 2015].

Teoreticky se zdá, že by federální úřady měly implementovat cloudová řešení ve velkém. Realita je však zatím výrazně odlišná. V roce 2014 vyšel report Vládního úřadu pro odpovědnost (GAO, Government Accountability Office), který se věnoval implementaci cloud computingu v 7 z 15 amerických ministerstev, a který navazoval na report z roku 2012. Dle tohoto reportu se za dva roky počet využívaných cloudových služeb zvýšil z 21 na 101. Na tyto služby se vydalo 530 mil. USD, tedy o nějakých 200 mil USD více než v předchozím období. Jedná se však o pouhá 2 % veškerých vynaložených prostředků na ICT. Hlavním důvodem takto nízkých čísel bylo, že ministerstva ignorovala využití cloudových služeb až pro cca 70% jejich ICT investic [GAO, 2014]. Cloudové služby byly zvažovány pouze pro ICT vybavení a služby, které se ocitly na konci svého životní cyklu a bylo je třeba renovovat - a to i přes to, že je to v rozporu s FCCS [FIGLIOLA, 2015].

Celkové úspory dosažené nasazením cloud computingu dosáhly 96 mil[11]. USD, což má velmi daleko k předpodkládaným 20 mld. USD, a přestože se nejedná o čísla všech federálních agentur.

Dalším zajímavým údajem je fakt, že tyto úspory přineslo pouze 22 z 101 implementací cloudu - ostatní služby tedy nevedly k přímým úsporám. Všechny cloudové služby však nebyly zaváděny z důvodu úspor, ale spíše kvůli vylepšení stávajících služeb. Dalšími benefity nasazení cloudu bylo snížení času nasazení služeb, zvýšení flexibility a zmenšení potřebné IT infrastruktury.

Mezi hlavními důvody malého využívání cloud computingu byly (kromě již zmíněných) federální požadavky na bezpečnost, které se v posledních dvou letech měnily, dále překonávání kulturních bariér (ve smyslu změny způsobu, jakým bylo dosud k IT službám přistupováno), nedostatečná či zastaralá síťová infrastruktura, nedostatek potřebných znalosti pro akvizici cloudových služeb a také nedostatek finančních prostředků pro implementaci.

Výše zmíněné důvody nevyužívání cloud computingu nepovažuje autor práce za specifické pouze pro USA, ale dají se z velké části aplikovat na celý veřejný sektor. Na příkladu USA je vídět, že ani jasně definovaná státní (v tomto případě federální) strategie není zárukou rychlého úspěchu implementace cloudových služeb, a i přes jasně stanovené povinnosti může

[11] Jako příklad si můžeme uvést nasazení cloudového řešení pro zákaznickou podporu nasazenou GSA (General Services Administration), na které bylo ušetřeno 2,6 mil USD. Přechod na cloud se ukázal jako levnější varianta než aktualizace stávajícího řešení.

narazit na odpor a nechuť veřejného sektoru čelit změnám, které sebou přechod na poskytování ICT jako služby nese.

2.2.3. Další evropské státy

Kromě celoevropských projektů, jako je Trusted Cloud for Europe, vzniká celá další řada národních iniciativ pro využití cloud computingu v rámci veřejného sektoru. Dle studie irské společnosti Accenture existují v rámci Evropské unie tři základní přístupy pro využívání cloud computingu veřejným sektorem: budovatelský, vylepšovatelský a spořící [ACCENTURE, 2013]. První z nich je tzv. „budovatelský" přístup, který zástavají především země střední a východní Evropy, jež spočívá v budování cloudové infrastruktury pro potřeby veřejné správy. Jedná se především o země střední a východní Evropy jako Maďarsko, Polsko, Slovensko (které počítá s velkými úsporami při přechodu na cloud [MF SR, 2012]) a jak již bylo popsáno i Česká republika.

Druhý přístup, označovaný jako „vylepšovatelský", spočívá v pomalejším začleňování cloudových služeb do již existující infrastruktury. Tímto přístupem se vyznačují země jako Rakousko, Dánsko, Belgie či Německo [ACCENTURE, 2013]. V Německu existuje platforma TrustedCloud, která slouží k podpoře spolupráce mezi zástupci veřejného a privátního sektoru s cílem vytváření cloudových služeb, které by byly v souladu s platnou německou legislativou a splňovaly všechny bezpečnostní požadavky pro jejich využití veřejným i privátním sektorem.

Poslední přístup je označovaný jako „spořící", jež vyznávají především země snažící se o co největší úspory. Zástupci tohoto přístupu jsou Francie, Itálie a především Velká Británie, jež je první evropskou zemí, která zavedla politiku „cloud-first". Na její přístup se podíváme blíže v následující podkapitole.

2.2.4. G-Cloud Velké Británie

G-Cloud je britská iniciativa pro usnadnění nákupu cloudových řešení institucemi veřejného sektoru.

S poskytovateli jednotlivých služeb jsou uzavřeny rámcové smlouvy, které obsahují předmět poskytované služby, cenu, všeobecné smluvní podmínky a další informace. Poskytovatelé pak mohou své služby nabízet na veřejně dostupném online tržišti[12] nazvaném stroze „Digital Marketplace" (dále Tržiště).

[12] Dostupné z https://www.digitalmarketplace.service.gov.uk.

Digitální tržiště obsahuje seznam všech dostupných služeb, jichž je cca 16.000 a jsou rozděleny do 4 kategorií (IaaS, PaaS, SaaS a Služby cloudových specialistů, kteří nabízejí pomoc s implementací, plánováním apod.), které se dělí na další podkategorie. Kromě toho obsahuje podrobné návody pro veřejný sektor, jak služby nakupovat a pro poskytovatele, jak služby nabízet. Na Tržišti je také dostupný seznam institucí, které takto mohou služby nakupovat.

Od spuštění provozu v roce 2012 do ledna 2015 bylo skrze tržiště zaplaceno za služby v celkové hodnotě 467.404.892,84 £, z čehož více než polovina byla zaplacena malým a střední podnikům [GOVERNMENT DIGITAL SERVICE, 2014]. To je sice poměrně malá část z celkového rozpočtu UK na ICT, jež se pohybuje okolo 10 mld. £ [LEACH, 2013], ale ne část zanedbatelná a má stále vzrůstající tendenci.

Britská strategie se, alespoň dle názoru autora, dá označit za poměrně úspěšnou. Příčiny tohoto úspěchu spočívají především ve dvou výhodách, jež mají instituce veřejného sektoru nakupující skrze Tržiště. Za prvé, při nákupu cloudových služeb z digitálního tržiště mají jistotu, že nabízené služby splňují bezpečnostní kritéria. Poskytovatelé musí vyplnit formulář, ve kterém se přihlašují k používání různých bezpečnostních prvků, které také musí následně doložit příslušnými certifikáty, jako jsou ISO 27001 či CSA Open Certification Scheme (VIZ KAP). Dle tohoto formuláře si uživatelé mohou následně ověřit splnění jimi požadovaných bezpečnostních prvků.

Druhou výhodou je zkrácení potřebného času pro akvizici služeb, neboť nemusejí vypisovat veřejné výběrové řízení. Kromě času tím také šetří nároky na administrativu a personál. Výběr služby však musí být řádně dokumentován a zdůvodněn pro případný audit. Vzhledem k přijaté politice „cloud-first", také musí být zdůvodněny případy, kdy instituce použijí „ne-cloudové" řešení.

2.2.5. Cloud computing v České republice

Na začátek je třeba říci, že v současnosti v ČR neexistuje žádná dosud přijatá strategie ani zvláštní podpora pro využívání služeb veřejného cloudu institucemi veřejného sektoru, tak jako je tomu v jiných zemích. A to i přes upozorňování na vhodnost využití cloudových služeb veřejným sektorem takovými orgány jako Národní ekonomickou radou vlády [NERV, 2011], ICT Unií a nejnověji také Radou vlády pro informační společnost (RVIS). To samozřejmě neznamená, že jednotlivé instituce by nemohly cloudové služby nasadit, ale jejich výchozí pozice je oproti jiným zemím, které takovou strategii zavedly, komplikovanější.

Ačkoliv neexistuje žádná strategie věnována přímo cloud computingu, některé strategické vládní dokumenty ho alespoň okrajově zmiňují nebo na možnosti využívání cloud computingu mají vliv. Těmito dokumenty, které si dále rozebereme, jsou:

- **Digitální Česko v 2.0 : Cesta k digitální ekonomice.**
- **Strategický rámec rozvoje veřejné správy České republiky pro období 2014 - 2020.**
- **Národní strategie kybernetické bezpečnosti České republiky na období let 2015-2020.**
- **Návrh opatření zvyšujících efektivnost služeb veřejné správy a podpůrných ICT služeb.**

Patrně nejzásadnějším je vládní dokument ***„Digitální Česko v 2.0 : Cesta k digitální ekonomice*"**. Digitální Česko v. 2.0 stanovuje 8 hlavních cílů vlády do roku 2020, jejichž naplnění má být zajištěno 17 opatřeními. Cloud computing je zde zmíněn a stručně rozebrán z hlediska svých výhod, ale o tom, zda se bude ČR snažit následovat strategii Evropské komise UPCCE pro rozvoj a využití cloudových služeb, se zde nedozvíme. Z opatření č. 10[13] však vyplývá, že stát by neměl (a neplánuje) regulovat žádnou novou technologii, pokud to nebude nutné [VLÁDA ČESKÉ REPUBLIKY, 2013].

Nejdůležitějším opatřením z hlediska cloud computingu, je opatření č. 3[14] slibující podporu rozvoje vysokorychlostních přístupových sítí k internetu umožňující přenosové rychlosti v souladu s cíli evropské Digitální agendy 30 Mbit/s do roku 2020 pro všechny obyvatele a 100 Mbit/s minimálně pro polovinu domácností. Kvalitní internetové připojení je nutnou podmínkou k využívání i poskytování cloudových služeb. Splnění tohoto opatření by z hlediska cloudu velice pozitivní [VLÁDA ČESKÉ REPUBLIKY, 2013].

Dalším strategickým dokumentem je „**Strategický rámec rozvoje veřejné správy České republiky pro období 2014 - 2020**" (dále Rámec 2020), zabývající se veřejnou správou a **e-governmentem,** jehož poslední a finální verze byla publikována v lednu 2015. Rámec 2020, navazující na Strategii Smart Administration, jež byla realizována od roku 2007 do 2015, má

[13] "*Ministerstvo průmyslu a obchodu bude sledovat a vyhodnocovat dopady využívání nových technologií v oblasti ICT a podporovat samoregulační mechanismy, neboť by nemělo být primárním cílem implementovat státní regulaci na jakoukoliv novou technologii. Zároveň vždy bude zkoumána zejména otázka bezpečnosti a spolehlivosti, ochrana soukromí, zabezpečení kritické infrastruktury (kybernetická bezpečnost), etiky, interoperability, řízení a technických norem. Stěžejní je pravidelný dialog mezi státní správou a soukromou sférou.*"

[14] "*Rada vlády pro konkurenceschopnost a informační společnost vypracuje návrh dalších opatření pro podporu výstavby NGA sítí, která se zaměří na využití veřejných zdrojů, zjednodušení administrativy spojené s výstavbou a na snížení poplatků spojených s věcnými břemeny. Tento návrh po veřejné konzultaci předloží vládě ke schválení.*"

stanovit další směr rozvoje české veřejné správy (včetně e-governmnetu) [MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2015].

Zde je třeba zmínit, že cloud computing byl dlouho považován za jeden z hlavních nástrojů pro budování služeb českého e-governmentu. Služby postavené na principech cloud computingu se v rámci českého e-governmentu označují jako „**sdílené služby**". První zmínky o cloud computingu pocházejí z roku 2011, kdy k **eGONovi**, figurce představující symbol českého e-governmentu, přibyla **Klaudia**, jež měla do českého e-governmentu zavést technologii cloud computingu a *„zajistit, aby byly ICT projekty nejen efektivnější a levnější, ale též umožnily přechod od současného stavu blížícího se správě majetku k modelu poskytování a odebírání služeb"* [MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2011]. V rámci českého e-governmentu se však nepočítalo s využitím služeb veřejného cloudu, ale v plánu bylo vytvoření privátního cloudu pro veřejnou správu. Některé státní podniky, jako Česká pošta, s.p., Odštěpný závod ICT služby či Státní tiskárna cenin, již cloudové služby nabízejí. Z části Státní tiskárny cenin by mělo vzniknout Národní datové centrum spadající pod Ministerstvo financí, které by poskytovalo IT služby pro státní instituce [ČTK, 2014].

Rámec 2020 však o sdílených službách nehovoří vůbec, a to i když byly součástí jeho starší verze z června 2014. Některé zprávy z poslední doby však naznačují, že se sdílenými službami, tedy cloud computingem, by se mohlo počítat i nadále.

Jednou z takových zpráv je dokument nazvaný „**Návrh opatření zvyšujících efektivnost služeb veřejné správy a podpůrných ICT služeb**" (dále Návrh), který byl poprvé představen 23. 1. 2015 na zasedání RVIS. RVIS byla ustanovena v listopadu 2014 a má sloužit jako poradní a koordinační orgán vlády pro oblast ICT a veřejné správy. Navazuje tak na zrušenou Radu vlády pro konkurenceschopnost a informační společnost, která byla zrušena před cca 2 roky. Koordinace v rukou jednoho nadresortního orgánu by jistě v této oblasti pomohla, protože situace, minimálně co se e-governmentu týče, je od doby zrušení Ministerstva informatiky a převzetí jeho kompetencí třemi jinými ministerstvy[15], značně nepřehledná a postrádající kontinuitu, což lze vypozorovat i z již zmíněných dokumentů.

Výše zmíněný Návrh nejprve shrnuje základní nedostatky současného stavu v oblasti řízení ICT veřejnou správou jako neexistence centrálního orgánu věnujícího se standardizaci ICT procesů, korupční prostředí v oblasti ICT zakázek veřejného sektoru a také právě minimální využívání cloud computingu (resp. sdílených služeb). V další části právě poskytuje návrhy

[15] Ministerstvo vnitra, Ministerstvo pro místní rozvoj a Ministerstvo průmyslu a obchodu.

pro zlepšení současného stavu. Jedním z navržených opatření je větší využívání sdílených služeb a to konkrétně *„zavést a udržovat centrální katalog sdílitelných certifikovaných ICT služeb*" [STROUHAL, 2014], který by měl mít podobu jako obdobné služby ve Velké Británii a USA (viz dvě předchozí podkapitoly). V jeho rámci by měly být poskytovány i služby soukromých firem, které by prošly zatím neurčenou certifikací. Jedná se tak o první zmínku podpory využívání služeb veřejného cloudu institucemi veřejného sektoru v ČR. V rámci tohoto opatření se zmiňuje i možnost zavedení politiky „cloud-first" pro veřejné instituce.

Z pohledu autora je však třeba zdůraznit, že samotný Návrh je v době psaní této práce skutečně pouhým návrhem a jednotlivé body navržené v tomto dokumentu se teprve budou projednávat a je otázkou, zda dojde k jejich schválení. Od případného uvedení do praxe je tak zatím velmi daleko.

Dalším strategickým dokumentem, který má vztah k využívání služeb veřejného cloudu je „**Národní strategie kybernetické bezpečnosti České republiky na období let 2015-2020"** (NSKB). Tento dokument navazuje na programové období let 2012-2015. Jednou z hlavních vizí NSKB je zajištění podmínek pro hladké fungovaní informační společnosti v kybernetickém prostoru[16], a to především z pohledu bezpečnosti - prevence a boje proti kyberkriminalitě [NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD, 2015.]. K tomu má sloužit vládní a národní CERT (Computer Emergency Response Team, tedy Reakční skupina na počítačové hrozby) a Zákon o kybernetické bezpečnosti který vstoupil v platnost 1. 1. 2015. Národní podpora zabezpečení kybernetického prostoru a boje proti kybernetické kriminalitě by měla mít pozitivní vliv i na využívání služeb cloud computingu, což potvrzuje např. i Business Software Alliance [2013].

Česká republika, jak se z výše uvedených poznatků zdá, momentálně stojí na rozcestí, které buď povede k podpoře využívání služeb veřejného cloudu, anebo zůstane u tvorby privátních řešení pro potřeby veřejné správy, případně celého veřejného sektoru. Cesta budování privátního cloudu nemusí být nutně cestou špatnou, ale nese značná rizika, která byla stručně zmíněna v úvodní kapitole. Je však také zřejmé, že ne všechna data mohou být svěřena do veřejného cloudu (více v legislativním okruhu PESTL analýzy).

[16] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti definuje kybernetický prostor jako "*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*"

V případě, že se zvolí cesta tvorby katalogu cloudových služeb dle Návrhu, by bylo vhodné zapojení zástupců České republiky do evropských iniciativ a pracovních skupin naplňujících strategie UPCCE (např. ECP), ve kterých zatím jakékoliv zastoupení ČR chybí.

2.3. Ekonomický okruh

O důvodech vzniku cloud computingu, které byly hnány především ekonomickými zájmy, jsme se již zmiňovali v úvodní kapitole. Analýze ekonomických dopadů využití cloudových služeb v institucích veřejného sektoru se bude věnovat SWOT analýza dále v textu.

V rámci této kapitoly, jež je součástí provedené PESTL analýzy, se zaměříme na modely zpoplatnění cloudových služeb. Stejně, jako je veliká variabilita cloudových služeb, tak se liší i způsoby, kterými se za tyto služby platí. Cloud computing přenáší velkou část nákladů na stranu provozovatelů, kteří by však měli být schopni své zdroje díky tzv. „úsporám z rozsahu[17]" využívat ekonomičtěji. Do ceny poskytované služby vstupuje celé řada faktorů, z nichž hlavní jsou počáteční náklady poskytovatele, doba pronájmu zdrojů uživatelem, kvalita služby (tzv. „QoS[18]") a náklady na údržbu.

Modelů zpoplatnění cloudových služeb existuje celá řada, některé zatím pouze v teoretické rovině. Zde si představíme 4 modely, se kterými se lze setkat v praxi a to model předplatitelský, spotřební, dynamický a reklamní.

Namístě je také popsat některé ekonomické termíny, které se s cloud computingem často pojí. Kromě již popsaných modelů zpoplatnění se jedná především o termíny TCO (Total Cost of Ownership, celkové náklady spojené s vlastnictvím), CAPEX (capital expenditures, investiční náklady) a OPEX (operational expenditures, provozní náklady), které poskytovatelé služeb často využívají pro popis ekonomických výhod cloud computingu (které budou podrobněji rozebrány ve SWOT analýze).

2.3.1. ICT výdaje veřejného sektoru

Zmapovat celkové výdaje veřejného sektoru na informační technologie a služby v ČR není lehký úkol, z veřejných informačních zdrojů spíše nereálný. Stát žádné statistiky v této oblasti nevydává a vzhledem k neexistenci nějaké centrální agentury pro nákup ICT je patrně ani nemá. Dá se tedy pouze vycházet z různých odhadů poradenských firem a oborových

[17] Z anglického termínu "economies of scale"

[18] Z anglického termínu 'Quality of Service', který v tomto případě označuje úroveň výkonu, spolehlivosti a dostupnosti. QoS by měla být jasně stanovena v rámci SLA.

organizací. Je také třeba doplnit, že údaj o tom, jakou částkou se na celkových nákladech podílí služby cloud computingu, je nezjistitelný.

Dle ČSÚ byl celkový roční objem ICT trhu za rok 2012 zhruba 634 mld. Kč [ČSÚ, 2012], z čehož 100 mld. Kč tvoří zakázky veřejného sektoru [KOUBSKÝ, 2011]. Naproti tomu společnost IDC odhadla pro rok 2012 objem zakázek veřejného sektoru (v tomto případě úřadů na centrální a regionální úrovni) na 13 mld. Kč [HERGESELL, 2014]. Ministerstvo financí v únoru 2015 publikovalo otevřené datové sady s údaji o ICT nákladech resortů ministerstev financí, obrany, místního rozvoje, životního prostředí, spravedlnosti a dopravy [MINISTERSTVO FINANCÍ ČESKÉ REPUBLIKY, 2015.]. Po sečtení všech nákladů za rok 2012 vychází celková částka na 4 mld. Kč. Za předpokladu, že zbylých 9 ministerstev má podobné výdaje, bychom došli ke konečné částce cca 10 mld. Kč. Odhady absolutních čísel se tedy značně liší (od 10 mld. do 100 mld. Kč). Zajímavější náhled na situaci přinášejí tedy čísla relativní.

Dle odhadu znaleckého ústavu Apogeo Esteem je 30 % - 35 % finančních prostředků na ICT vynakládáno neefektivně či přímo zbytečně [APOGEO, 2011]. To do jisté míry dokládají i statistiky IDC, podle kterých veřejný sektor vynaloží v průměru na jednoho občana 61,6 USD, což je jeden a půlkrát vyšší výdaj než na Slovensku a dvakrát více než je vydáváno v Polsku a Maďarsku [HERGESELL, 2014]. Příčin tohoto neefektivního nakládání s finančními prostředky je více. Některé, jako neexistence centrálního úřadu s dozorem nad ICT a další problémy spojené s (nestálou) politickou vizí využití ICT prostředků, byly již zmíněny a některé další, jako nedostatek ICT odborníků ve veřejném sektoru, budou popsány v následujících kapitolách. Apogeo ESTEEM poskytuje další důvody pro tuto neefektivitu: *„Viníkem je nejčastěji nedostatečná analýza projektů (25 %) vedoucí k jejich prodražování. Hned v závěsu je chybné zadání projektu (18 %), které poptává neadekvátní řešení"* [APOGEO, 2011]. Neadekvátním může být například předimenzované řešení, jež pak není využívané v předpokládaném rozsahu. Dalším faktorem negativně ovlivňujícím ICT náklady veřejné správy je i korupce, což potvrzuje ve své zprávě i Ministerstvo vnitra [STROUHAL, 2014].

Cloud computing není technologií, která by sama o sobě mohla vyřešit neduhy nakládání s veřejným prostředky, ale v některých oblastech má potenciál situaci alespoň vylepšit, což je podrobněji rozebráno v rámci SWOT analýzy.

2.3.2. Možnosti financování cloudových služeb ve veřejném sektoru

Základní možností financování využití cloud computingových služeb je z vlastních zdrojů instituce. Druhou možností, na kterou se v rámci této podkapitoly zaměříme, je využití některých dotačních fondů Evropské unie. Fondy EU slouží k financování cílů politiky EU, které jsou v současnosti stanoveny strategií „Evropa 2020" [MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR, 2014].

Pro financování cloud computingu ve veřejném sektoru případají v úvahu prostředky poskytované z „Evropských strukturálních a investičních fondů" (ESIF) a prostředky dostupné skrze tzv. rámcové programy pro vědu a výzkum [PETERKA, 2012a].

Evropské strukturální a investiční fondy

Prostředky z těchto ESIF fondů jsou poskytovány prostřednictvím jednotlivých operačních programů, které určují, na co mohou být finanční prostředky využity. Operační programy jsou vypisovány vždy na 7leté období - nyní pro roky 2014-2020.

Pro financování cloudových služeb lze využít „Integrovaný regionální operační program", konkrétně jeho třetí prioritní osy „Dobrá správa území a zefektivnění veřejných institucí" a specifického cíle této osy „zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT" [CYRRUS ADVISORY, 2015], pro který je alokováno 282,1 miliónů EUR.

V době psaní této práce nejsou však známy některé důležité informace, např. o jak vysokou spoluúčast bude možné žádat a ani žádné konkrétní výzvy, v jejichž rámci lze žádat o dotaci.

Je však také třeba zdůraznit, že programy vypisované v rámci ESIF podporují investiční projekty. Jejich využití je tedy limitováno na investiční náklady, jež jsou právě jednou z věcí, které by mělo využití služeb veřejného cloudu eliminovat. Lze je tedy použít na jednorázové náklady, které by mohly být spojeny s přechodem na cloudové služby. Případně jejich využití pro výstavbu řešení na bázi privátního cloudu. Tato řešení však nejsou objektem této diplomové práce.

Vzhledem k podpoře, jakou Evropská unie věnuje cloudovým službám, je trochu s podivem, že tento rozpor, kdy prakticky nelze z fondů financovat provozní náklady, nebyl nijak vyřešen.

Rámcové programy pro vědu a výzkum

Rámcový program pro vědu a výzkum pro období 2014-2020 nese název Horizont 2020. V pořadí je již osmým rámcovým programem a, co se finančních prostředků týče, je také nejvíce

dotovaným. Pro financování Horizontu 2020 bylo vyhrazeno 80 mld. EUR [EUROPEAN COMMISSION, 2014b]. Horizont 2020 slouží k financování výzkumných projektů a také k tvorbě a případnému nákupu inovativních řešení pro oblasti relevatní strategii Evropa 2020.

Horizont 2020 je rozdělen na tři základní pilíře, ze kterých je pro financování výzkumných či inovativních cloud computingových projektů ve veřejném sektoru zaměřen okruh „Informační a komunikační technologie" vedený v rámci pilíře „Vedoucí postavení evropského průmyslu". V rámci tohoto okruhu jsou vypisována různá témata specifikující oblasti, ve kterých mohou instituce veřejného sektoru žádat o grantovou podporu.

Oblastí určenou pro cloud computingové služby je 8. téma nazvané „Podpora inovace a produktivity veřejného sektoru prostřednictvím služeb cloud computingu". V jeho rámci mohou veřejné instituce zadávat zakázky v předobchodní fázi (PCP, pre-commercial procurement, o kterých je více dále v textu) na vývoj nových cloudových řesení či přímo zadávat veřejné zakázky na akvizici již existujících (inovativní) cloudových služeb [EUROPEAN COMMISSION, 2014a].

Tento program má však 2 podstatná omezení. Prvním z nich je, že zadávání obou typů veřejných zakázek musí provést společně nejméně tři instituce ze tří různých zemí [EVROPSKÁ UNIE, 2013] zařazených do programu (spolupráce není omezena pouze na členské země EU), čímž má být zajištěn celoevropský dopad tohoto programu. Druhým omezením je to, že podávání návrhů v rámci 8. tématu končí již 14. dubna. Tedy v době publikace této diplomové práce již nebude aktuální. Avšak dá se s jistotou očekávat, že stejné nebo podobné téma bude opět vypsáno. A vzhledem k tomu, že výsledky vzešlé ze zakázek zadaných v předobchodní fázi mají sloužit k uvedení nového výrobku (služby) na trh, by se sledování výstupů z tohoto okruhu mohlo institucím veřejného sektoru vyplatit.

2.3.3. Veřejné zakázky v předobchodní fázi

Jedním z možných způsobů pro poptávání cloudových služeb je také využití zadávání veřejných zakázek v předobchodní fázi (PCP), jež je definováno jako *„proces, kterým veřejné organizace mohou řídit od počátečního stádia vývoj inovačních technologií a služeb, které umožní řešit jejich specifické potřeby* [POKORNÝ, 2013]".

Nejedná se tedy o poptávání již hotových řešení, ale veřejné instituce si samy definují požadavky na nové řešení (tedy takové, které ještě není dostupné na trhu) a pomocí výběrového řízení hledají společnosti (veřejné i soukromé) zabývající se výzkumem a vývojem, které budou schopné (a ochotné) takové řešení vyvinout. PCP stojí na několika prinicipech, které mají zajistit jejich výhodnost pro všechny zúčastněné strany. Především se

jedná o sdílení rizik, duševního vlastnictví, ale i případných zisků vzešlých z uvedení daného řešení na trh. Konečným uživatelem nemusí být pouze zadavatel, ale počítá se právě i s uvedením daného řešení na trh [EVROPSKÁ KOMISE, 2007].

Využívání PCP je součástí strategie Evropa 2020 a má sloužit k zvýšení inovačního potenciálu EU a zároveň zvýšit celkovou kvalitu a účinnost veřejných služeb. PCP pro cloud computingové služby veřejného sektoru je podporováno granty poskytovanými v rámci programu EU Horizont 2020.

V ČR zatím neexistuje žádný program pro podporu využívání PCP a zkušenosti s jejich zadáváním jsou minimální. První veřejná zakázka zadaná metodou PCP byla vyhlášena teprve 27. 2. 2014 [TECHNOLOGICKÁ AGENTURA ČR, 2014]. Vzhledem k tomu, že EU podporuje implementaci národních PCP projektů, by se však tento stav mohl brzy změnit. PCP projekty již běží v různém rozsahu například ve Velké Británie, Nizozemí, Maďarsku a Polsku.

Autorovi se PCP jeví jako zajímavý a nadějný způsob získávání nových služeb na bázi cloud computingu vhodných pro veřejný sektor, i když z praktického hlediska půjde o náročný proces.

2.3.4. Modely zpoplatnění cloudových služeb

- **Předplatitelský model**

  V tomto modelu jsou všechny služby nabízeny za fixní poplatky. Ty mohou být stanoveny dle různých kritérií jako počet uživatelů (cena za uživatele), doba používání (cena za den/měsíc/rok), či předem stanovený rozsah využívaných služeb jako velikost datových úložišť (cena za 1GB) [AL-ROOMI, 2013].

  Jednoznačnou výhodou tohoto modelu je, že částka, která bude za služby zaplacena je známa předem. Z praktického hlediska se zatím jedná o nejlépe využitelný model zpoplatnění cloudových služeb pro veřejné instituce, jež se musí řídit zákonem č. 137/2006 Sb, o veřejných zakázkách.

  Z hlediska poměru mezi cenou a výkonem se pro uživatele může jednat o model jak výhodný, tak nevýhodný. Záleží především na míře využití poskytovaných služeb. Čím větší využití, tím se uživatelské instituci tento model vyplatí mnohem více, než pokud bude služba využívána málo a bude tak placeno převážně za čas, kdy služba nebyla využívána.

- **Spotřební („pay-as-you-go") model**

Služby jsou zpoplatněny zpětně dle skutečné spotřeby, která je určená pomocí měřících mechanismů poskytovatele služby (tzv. pay-as-you-go/pay-as-you-use model), jež musí být uživateli samozřejmě známy dopředu a jasně stanoveny v rámci SLA. Tento model účtování poplatků za využité služby bývá označován jako jedna z hlavních vlastností a novinek, které cloudové služby přinesly [LEIMBACH, 2014].

Měřené služby se mohou značně lišit dle druhu poskytované služby. Tento model bývá využíván zejména v prostředí IaaS a PaaS, v jejichž rámci to mohou být data přenesená přes síť, využité místo v datových úložištích, počet přidělených IP adres a podobně.

Nevýhoda tohoto modelu spočívá v těžké odhadnutelnosti konečných nákladů pro uživatele. Tento model také vyžaduje větší nároky na uživatele, kteří musí zdroje využívat s rozvahou. Výhodou spotřebního modelu je placení za skutečně využité zdroje.

Dynamický model

Dynamický model zahrnuje aukce, reverzní aukce či spotové trhy. Označení dynamický vychází z toho, že ceny jsou průběžně měněny. V praxi tento model není příliš rozšířený.

Jako příklad lze uvést službu Amazon EC2 Spot Instances. Ta dovoluje uživatelům přihazovat na nevyužité prostředky, a ve chvíli, kdy nabídnutá cena přesáhne cenu požadovanou provozovatelem je služba poskytnuta. Cena za služby se dynamicky mění na základě nabídky a poptávky.

Tento model však evidentně není příliš vhodný pro využití ve veřejném sektoru, a to z důvodů značné složitosti a nepředvídatelnosti.

- **Reklamní model**

Je uplatňován především pro cloudové služby, které nejsou zpoplatněny, ale jsou financovány reklamou, která je zobrazována uživatelům služby. Častý model je, že základní služba je poskytována zdarma (s reklamou), ale je možné zaplatit za nadstandardní služby.

Reklamní model je využíván některými službami SaaS, jako jsou například sociální sítě. Ty jsou, i v rámci veřejného sektoru, často používány jako jeden z komunikačních kanálů s konečnými uživateli. Jejich využití patrně nic nebrání, ale je třeba se podrobně seznámit s podmínkami využití těchto služeb.

Pro využití ve veřejném sektoru se nejlépe využitelný zdá model předplatitelský (a do jisté míry také reklamní), protože jeho finanční náklady lze poměrně lehce odhadnout a stanovit v rámci zadávací dokumentace výběrového řízení (vysvětleno dále v textu). Zde je také třeba

upozornit na fakt, že do dubna roku 2016 by mělo dojít k implementaci přepracovaných evropských směrnic 2004/17/ES a 2004/18/ES, upravujících zadávání veřejných zakázek, do české legislativy, jež by mohla ulehčit zadávaní veřejných zakázek a zjednodušit tak využití i dalších platebních modelů cloudových služeb pro veřejný sektor, což se, vzhledem k podpoře EU pro využívání cloud computingu, jeví realisticky.

2.3.5. Základní ekonomické termíny

Celkové náklady vlastnictví (TCO)

„Celkové náklady vlastnictví" (dále TCO, Total Cost of Ownership) je metoda vyvinutá společností Gartner pro analýzu ICT nákladů organizace (ačkoliv její využití je univerzálnější). Gartner [2005] definuje TCO jako holistický pohled na náklady, vztahující se ke zkoumanému aspektu, napříč celou organizací vzniklých v průběhu času. Metoda se dá uplatnit jak na náklady veškerého ICT vybavení, tak na jedno konkrétní zařízení či službu.

V rámci výpočtu nákladů metodou TCO musí být započítány přímé i nepřímé náklady vynaložené v průběhu celého životního cyklu zkoumaného ICT zdroje. Pro výpočet TCO se sestavuje tabulka všech elementů, které se podílí na celkových nákladech. Těmito elementy mohou být:

- Náklady na HW a SW
- Mzdy pracovníků
- Náklady na údržbu a technickou podporu
- Náklady na energie spojené s provozem
- Náklady na školení pracovníků
- Administrativní náklady
- Náklady na migraci atd.

Kapitálové náklady (CAPEX)

Kapitálové neboli investiční náklady (označované zkratkou CAPEX, z angl. capital expenditures) vznikají při koupi nového nebo aktualizací stávajícího zařízení. Kapitálové náklady jsou jednorázové.

Provozní náklady (OPEX)

Provozní náklady (označované zkratkou OPEX, z angl. originálu operational expenditures) zahrnují všechny nutné náklady pro udržení stávajícího zařízení v chodu. Na rozdíl od CAPEX jsou provozní náklady průběžné a opakující se.

2.4. Sociální okruh PESTL Analýzy

V rámci 3. okruhu PESTL analýzy jsou rozebrány některé faktory vlivu sociální sféry, především lidského kapitálu a jeho vlivu na využití cloudových služeb ve veřejném sektoru. V první části je analyzováno postavení odborníků pro oblast informačních technologií na trhu práce a jejich uplatňování ve veřejném sektoru. Druhá část tohoto okruhu stručně hodnotí možnosti využití e-governmentu občany ČR. Poslední část je věnována představení výsledků průzkumu, provedeného společností IDC, zaměřeného na vztah veřejného sektoru k využití cloudových služeb.

2.4.1. ICT odborníci ve veřejném sektoru

Pro provoz ICT infrastruktury organizace jsou potřeba ICT odborníci, kteří patří dlouhodobě k nejlépe placeným oborům. Ve veřejném sektoru se však jejich finanční hodnocení pohybuje okolo 60 % toho, co mohou dostat v sektoru soukromém. To, jak ve svém reportu upozorňuje RVIS, vede k nedostatku kvalitních ICT odborníků ve veřejném sektoru [STROUHAL. 2014]. Pro úplnost, dle statistiky Českého statistického úřadu, je v ČR cca 150.000 ICT odborníků, z nichž 5 % pracuje ve veřejném sektoru [ČESKÝ STATISTICKÝ ÚŘAD, 2014].

Nedostatek ICT odborníků je problém celoevropský. Dle předběžných odhadů mělo být v roce 2015 cca 900 000 neobsazených pracovních míst vyžadujících ICT odborníky, což je vzrůstající trend oproti předchozím rokům[EVROPSKÁ KOMISE, 2013a]. Z toho se dá usuzovat, že pro veřejný sektor bude získání kvalifikovaných ICT odborníků stále obtížnější, a to s ohledem na výše zmíněné platové podmínky ve veřejném sektoru.

Pozitivní změna se v tomto ohledu v blízké době patrně nedá očekávat, neboť v roce 2014 až 70 % organizací veřejného sektoru muselo snižovat rozpočet na ICT a o dva roky dříve jich tak musela učinit polovina. K tomu je také třeba dodat, že až 80 % ICT rozpočtu organizací veřejného sektoru jde na provozní výdaje (jako údržba apod.) [DELOITTE, 2014].

S využitím služeb veřejného cloudu nemizí potřeba interních ICT odborníků, ale mění se náplň jejich činnosti. Ta již nemusí být soustředěna tolik na udržení provozu ICT

infrastruktury, ale může být směřována více k inovacím a celkovému zlepšování poskytovaných služeb.

2.4.2. Společnost a digitální ekonomika

Evropská unie využívá souhrnný index DESI (The Digital Economy and Society Index) pro shrnutí relevantních indikátorů ukazujících výkonnost jednotlivých členských států EU v oblasti digitální ekonomiky a digitální konkurenceschopnosti [EVROPSKÁ KOMISE, 2015a].

V indexu DESI je zahrnuto 5 indikátorů, kterými jsou: připojení k Internetu; lidský kapitál (schopnost občanů využívat informační technologie); využívání Internetu; integrace digitálních technologií (ve smyslu využívání digitálních technologií firmami); a indikátor poskytování digitálních služeb veřejnosti ze strany veřejného sektoru (např. e-government).

V celkovém hodnocení za rok 2014 se ČR umístila na 17. pozici s hodnocením pod průměrem EU. Je tedy zřejmé, že existuje dost prostoru ke zlepšení. ČR si stojí dobře především v oblasti lidského kapitálu, kde je v rámci EU hodnocena nadprůměrně. Více než 76 % občanů[19] ČR je pravidelnými uživateli Internetu a 56 % občanů má alespoň základní digitální schopnosti20. Tyto statistiky tedy vcelku jasně ukazují, že v ČR je poměrně velký lidský potenciál pro využívání digitálních služeb veřejného sektoru.

ČR, dle indexu DESI, v oblasti e-governmentu velice zaostává a v celkovém hodnocení se umístila na 25. místě. Zkoumanými oblastmi tohoto indikátoru jsou zaměření na uživatele (zda a jak jsou služby dostupné online), transparentnost veřejné správy (s ohledem na vlastní povinnosti či práci s osobními údaji), přeshraniční mobilita (do jaké míry mohou občané využívat služby veřejné správy z jiných zemí), klíčové předpoklady (elektronická identifikace, bezpečnost, single-sign on prostředí atd.) a některé další. V žádné z těchto oblastí ČR nedosahuje ani evropského průměru.

Tento stav se odráží i na skutečném výkonu veřejné správy, jež je, jak ukazuje průzkum EU, ve špatném stavu. Cloudové služby nejsou nástrojem, který by mohl sám o sobě vyřešit neduhy českého e-governmentu, ale mohou poskytnout prostředky pro jeho zlepšení.

[19] Ve věku 16-76 let.

[20] Na první pohled nelogický nepoměr, ale základní digitální schopnosti zahrnují také aktivní schopnosti jako tvorbu obsahu, provádění transakcí (např. nákup zboží) apod. Tedy i občan nesplňující kritéria pro základní digitální schopnosti může být uživatelem Internetu.

2.4.3. Vnímání cloud computingu veřejným sektorem

Americká společnost „International Data Corporation" (IDC) zabývající se průzkumem trhu provedla v roce 2011 výzkum mezi organizacemi soukromého i veřejného sektoru v EU, jež byl zaměřený na bariéry stojící v cestě využívání cloud computingu [CATTANEO, 2012]. Veřejný sektor byl zastoupen 239 respondenty z vládních, zdravotnických a vzdělávacích institucí (oproti 817 respondentům ze soukromé sféry).

Jako hlavní bariéry pro využívání cloud computingu institucemi veřejného sektoru byly identifikovány:

Bezpečnost a ochrana dat, jež byla veřejným sektorem vnímána jako nejdůležitější faktor.

Ohodnocení užitečnosti cloudových služeb pro potřeby organizace, se kterým si veřejný sektor (dle této studie) neví příliš rady, byl ohodnocen jako druhý nejdůležitější faktor.

Rozhodné právo, geografické umístění dat, jejich dostupnost a přenosnost následovaly jako další důležité překážky pro přechod ke cloudovým službám.

Dalšími, avšak ne tak důležitými negativními faktory z pohledu veřejného sektoru, byly jazyková lokalizace cloudových služeb, otázky ohledně duševního práva k případným úpravám (customisation) cloudových služeb. Tyto bariéry a možné způsoby jejich překonání jsou součástí SWOT analýzy provedené v rámci této diplomové práce.

Žádné průzkumy vztahu českého veřejného sektoru ke cloud computingu nebyly provedeny nebo nejsou veřejně dostupné.

2.5. Technologický okruh

Samotné technologické základy cloud computingu byly již popsány v úvodní kapitole. V rámci technologického okruhu PESTL analýzy se zaměříme na technické standardy v oblasti cloud computingu a certifikáty, které potvrzují jejich využívání poskytovateli. Dále také bude analyzována situace v oblasti internetového připojení v ČR, jež je základní podmínkou pro možnost využívání cloudových služeb.

2.5.1. Připojení k Internetu v ČR

Připojení k Internetu je zcela nutnou podmínkou využívání služeb veřejného cloudu. Pro plné využití potenciálu je třeba kvalitního širokopásmového připojení (tzv. broadband). Širokopásmové připojení je definováno jako připojení s vyšší přenosovou kapacitou než 1,5 nebo 2 Mbit/s [ITU, 2004]. Technologicky není omezeno a pokrývá tedy jakékoliv připojení s danou přenosovou kapacitou, ať už se jedná o drátové (např. ADSL, Asymmetric Digital Subscriber Line) či bezdrátové (např. Wi-Fi) připojení.

Dostupnost širokopásmového připojení v ČR je v rámci EU lehce nad průměrem. V rámci hodnocení indexu DESI se ČR umístila na 14. místě. Širokopásmové připojení bylo na konci roku 2013 dostupné pro 99 % domácností (v mimoměstských oblastech pro 91 %). Z toho 64 % připojení patří mezi tzv. přístupové sítě nové generace (NGA, New Generation Access), které poskytují přenosovou rychlost 30 Mbit/s a vyšší [EVROPSKÁ KOMISE, 2015b]. Reálně bylo dle Českého statistického úřadu (ČSÚ) připojeno k Internetu 70 % domácností v roce 2014. Průměrná rychlost připojení v ČR je cca 12 Mbit/s, což ČR řadí na 9. místo celosvětově [AKAMAI, 2014]. Poněkud horší situace je u mobilního připojení 4. generace (tzv. LTE, Long-Term Evolution), jež bylo v roce 2014 dostupno pro 12 % populace ČR.

Pokrytí veřejného sektoru bylo do roku 2011 zkoumáno ČSÚ a aktuálnější data nejsou momentálně dostupná. Vysokorychlostní připojení k Internetu, což je dle definice ČSÚ jakékoliv připojení s přenosovou kapacitou vyšší než 256 kbit/s (tedy pouhých 0,256 Mbit/s), bylo dle posledního průzkumu zavedeno ve všech krajských úřadů, 99,8 % organizačních složek státu a 88,2 % obecních úřadů [ČSÚ, 2014]. V rámci veřejné správy je také provozována KIVS (komunikační infrastruktura veřejné správy), jež má propojovat subjekty veřejné správy mezi sebou, a případně i s okolními „vládními“ sítěmi jiných států, a také sloužit jako intranet veřejné správy [PETERKA, 2012b]. Budování KIVS začalo v roce 2011 s cílem „*vytvoření jednotné datové sítě, která poskytne bezpečné připojení a vysoký standard nabízených služeb. Druhým cílem bylo odstranění monopolu poskytovatelů datových služeb*“. Konkrétní informace o propojení jednotlivých subjektů, přenosné kapacitě apod. však nejsou z veřejných zdrojů dostupné.

Na základě výše uvedených informací si autor dovoluje vyslovit názor, že infrastruktura pro připojení k Internetu v ČR je na dobré úrovni, ačkoliv průběžné zlepšování (zejména v dostupnosti kvalitního mobilního připojení) bude nadále nutné. Infrastruktura internetového připojení by tak neměla mít negativní vliv na možnost využívání služeb veřejného cloudu v ČR. Přesto je třeba vždy zhodnotit konkrétní situaci. Cloud computing klade vysoké nároky na propustnost dat směrem dovnitř (download) i ven (upload) z organizace. Současná situace s připojením k Internetu a její možné vylepšení v případě nutnosti, tak musí být bráno v potaz na úrovni jednotlivých institucí veřejného sektoru.

2.5.2. Standardizace a cloud computing

Specifikací a standardů pro cloud computing existuje celá řada (viz níže). Situace je na první pohled značně nepřehledná. Evropská komise ji ve svém strategickém dokumentu UPCCE dokonce nazvala džunglí, tuto tezi však vyvrací studie provedená ETSI [2013].

Standardizační činnost je sice rozprostřena mezi mnohé subjekty (viz níže), ale pole jejich působností se příliš, až na výjimky, nepřekrývají.

Standardizace v oblasti cloud computingu má pro širší využívání jeho služeb nesporné výhody. Jedním z nejčastěji zmiňovaných rizik při využívání cloudových služeb je přílišná závislost, či přímo uzamknutí se u jediného poskytovatele („vendor lock-in", vysvětleno ve SWOT analýze) [AMBRUST, 2009]. Uživatelé potřebují mít možnost vyjmout či převést svá data a aplikaci k jinému poskytovateli. Jednou z obran proti tomuto jevu je využívaní cloudových služeb, které podporují interoperabilitu s jinými službami. A interoperabilita mezi různými systémy je podmíněna využíváním mezinárodních (otevřených) standardů při jejich tvorbě. Nízká či dokonce žádná interoperabilita však není jedinou překážkou pro využívání cloudových služeb a ani jediná oblast řešená standardizací.

Vytváření otevřených standardů pro cloud computing se chopila celá řada subjektů od mezinárodních organizací zabývajících se standardizací až po konsorcia největších poskytovatelů cloudových služeb[21].

Mezinárodní organizace:

- **Mezinárodní organizace pro normalizaci** (ISO, *International Organization for Standardization*)
- **Mezinárodní elektrotechnická komise** (IEC, *International Electrotechnical Commission*),

  ISO a IEC společně vydaly standardy pro terminologii cloud computingu (ISO/IEC 17788:2014), referenční architekturu (ISO/IEC 17789:2014), ochranu osobních dat v cloudu (ISO/IEC 27018:2014, více info dále v textu) a dále pracují na standardech pro tvorbu SLA a standardech zabývajících se interoperabilitou.
- **Mezinárodní telekomunikační unie** (ITU, *International Telecommunication Union*)

  Zabývá se především oblastí bezpečnosti cloudových služeb (Recommendation X.1601)
- **Evropský ústav pro telekomunikační normy** (ETSI, *European Telecommunications Standards Institute*)

  Její činnost zahrnuje normalizaci v oblasti interoperability (norma ETSI TS 103 142) a doporučení pro cloudové SLA (ETSI TR 103 125)

[21] Ta nepatří mezi formálně uznané organizace pro vývoj standardů. Přesto jsou to značně autoritativní organizace v oblasti cloud computingu.

- **Evropská agentura pro bezpečnost sítí a informací** (ENISA, *European Network and Information Security Agency*)

  ENISA se podobně jako ETSI zabývá bezpečnostní cloudových služeb, ale také publikuje studie věnující se využití cloud computingu na vládní úrovni [ENISA, 2015]

Další organizace:

- **Cloud Security Alliance** (CSA),

  CSA je nezisková organizace, jejíž hlavní oblastí působnosti je bezpečnost cloud computingu a také vydávání certifikací pro poskytovatele cloudových služeb, organizace

- **OASIS** (*Organization for the Advancement of Structured Information Standards*)

  Organizace pracující na standardech pro správu identit v cloudu a standardizovaných požadavcích na cloudové služby pro veřejnou správu.

- **Open Grid Forum** (OGF)

  Mezinárodní organizace sdružující poskytovatele služeb, uživatele a vývojáře. Původně zaměřená především na gridové systémy, ale v současnosti se též věnuje cloud computingu. Její činnost pokrývá tvorbu standardů pro interoperabilitu cloudových služeb a především vytváří nástroj „Open Cloud Computing Interface" pro správu cloudových služeb umožňující interoperabilitu a přenositelnost dat.

  Nadace OpenStack původně založená NASA[22]a nyní tvořena zástupci největších IT společnostní (IBM, Dell, Hewlett-Packard), která vyvíjí nástroj OpenStack určený pro tvorbu a správu otevřených cloudových systémů.

  Z tohoto stručného přehledu organizací pracujících na standardizaci cloudových technologií je vidět, že cloud computing by se v následujících letech měl stále více standardizovat, a to zejména v oblasti bezpečnosti a interoperability. Na to bude mít velký vliv také to, jak moc budou zákazníci po poskytovatelích standardizované služby vyžadovat. A největším zákazníkem (= nejvíce platícím) v oblasti IT jsou instituce veřejného sektoru (resp. veřejný sektor jako takový).

2.5.3. Certifikační schémata cloudových služeb

Jedna věc je existence standardů a druhá je jejich skutečné využívání v praxi. Uživatelé se přechodem na cloud computing vzdávají dohledu nad částí svých IT prostředků (v závislosti

[22] National Aeronautics and Space Administration *(*Národní úřad pro letectví a kosmonautiku)

na využitém servisním modelu) a potřebují tedy záruky, že poskytované služby odpovídají určitým standardům. Ověřit vlastními silami, že služba odpovídá požadovaným standardům pro bezpečnost, spolehlivost, interoperabilitu a dalším důležitým parametrům není obvykle v možnostech jednotlivých uživatelů. Nejlepším vodítkem pro ověření, že poskytovatel (případně jeho jedna konkrétní služba) odpovídá požadavkům, jsou certifikace. Ty jsou obvykle udělovány na základě auditu nezávislé třetí strany, který má potvrdit, že daná služba/poskytovatel splňují požadavky daného certifikačního schématu. Existuje také druhá varianta certifikace, jež spočívá v tom, že poskytovatelé „certifikují" sami sebe, respektive přihlásí se k používání patřičných standardů.

Instituce veřejného sektoru mohou do zadávací dokumentace výběrového řízení (jeho význam je vysvětlen v příští podkapitole) zanést požadavky na certifikace, jejichž držitelem musí být případný zájemce o zakázku. V současnosti existuje několik relevantních certifikačních schémat pro veřejné cloudové služby. Těmi jsou:

- ISO/IEC 27001
- ISO/IEC 27017
- CSA Open Certification Scheme (CSA OCS)
- EuroCloud Star Audit (ECSA)
- Certified Cloud Service - TÜV Rheinland (CCS)
- TRUSTed Cloud Data Privacy Certification (TRUST)
- Service Organization Control 1-2-3 (SOC 1-2-3)
- EuroPriSe
- Federal Information Security Management Act - FISMA
- FedRamp

Daná certifikační schémata lze dělit podle různých kritérií, např. dle geografického působení (mezinárodní - ISO/IEC 27001, 27017, CSA OCS, ECSA, TRUST, SOC 1-2-3 X národní - americký FedRamp a FISMA, německý CCS) či zaměření schémat (bezpečnost - ISO/IEC 27001, CSA OCS, FedRamp X soukromí - TRUST, ISO/IEC 27017, EuroPriSe X všeobecné ECSA, CCS).

Na následujících řádcích si blíže představíme 4 z výše zmíněných schémat, a to ISO/IEC 27001 a 27018, které patří do rodiny standardů ISO/IEC 27000 a dále schémata CSA OCS a ECSA.

Rodina standardů ISO/IEC 27000

Rodina standardů ISO/IEC 27000, publikovaná společně organizacemi ISO a IEC, je zaměřená na bezpečnost informací v organizacích. Z pohledu uživatele cloudových služeb jsou v současnosti nejzásadnější normy ISO/IEC 27001, 27002, 27018 a brzy by se měla přidat také norma ISO/IEC 27017.

Norma ISO/IEC 27001 (revidována v roce 2013) stanovuje požadavky na ustanovení, implementaci, provoz a zlepšování systému řízení bezpečnosti informací (dále jen ISMS, *Information Security Management System)*. ISMS má sloužit k zachování důvěrnosti (k informacím mají přístup pouze autorizované osoby), integrity (uchování celistvosti a přesnosti) a dostupnosti informací pomocí procesu řízení rizik v rámci organizace [ISO, 2013a].

Požadavky stanovené normou ISO/IEC 27001 se naplňují dle normy ISO/IEC 27002, která poskytuje detailní popis různých bezpečnostních opatření, které je možné využít pro zavedení ISMS. Organizace jsou certifikovány dle normy ISO/IEC 27001.

ISO/IEC 27001 je v současnosti nejznámější a nejrozšířenější standard a certifikace v oblasti informační bezpečnosti (v roce 2013 bylo celosvětově certifikováno přes 22.000 organizací [ISO, 2013b]). Výhodou tohoto standardu je do jisté míry značná kompatibilita s požadavky stanovenými zákonem o kybernetické bezpečnosti [KRÁTKÝ, 2014], který bude rozebrán v následující podkapitole.

Norma ISO/IEC 27018, publikována v roce 2014, je zaměřená na ochranu osobních údajů v cloudu. Norma poskytuje instrukce pro poskytovatele veřejných cloudových služeb založené na normě ISO/IEC 27002, kterou rozšiřuje právě o popis požadavků na zabezpečení osobních údajů. ISO/IE 27018 je určena pro všechny typy organizací (malé, velké, soukromé, veřejné), které se mohou dostat do role poskytovatelů.

ISO/IEC 27018 zohledňuje požadavky na zpracovávání osobních údajů v cloudu stanovené směrnicí 95/46/ES.

V současnosti se jedná o stále nový standard, na jehož základě je certifikováno naprosté minimum poskytovatelů/služeb (v současnosti to jsou například některé cloudové služby

Microsoftu jako platforma Azure či kancelářský software Office 365). Vzhledem k popularitě a kredibilitě ISO standardů se dá však očekávat nárůst takto certifikovaných služeb/poskytovatelů.

Norma ISO/IEC 27017 bude doplňovat ISO/IEC 27002 o instrukce pro nasazení ISMS v cloudovém prostředí. Její součástí by měla být instrukce jak pro poskytovatele, tak uživatele cloudových služeb. Momentálně je stále ve vývoji, ale první verze by mohla být publikována již v polovině roku 2015 [ISECT, 2015].

Certfikace na základě ISO standardů jsou udělovány nezávislými auditory, tzv. certifikačními orgány. Samotná organizace ISO se na ní nijak nepodílí. Každá země má svoji národní akreditační agenturu, která akredituje certifikační orgány, které mohou dále certifikovat organizace či některé jejích služby. Certifikační proces se musí každé tři roky opakovat, což zaručuje dodržování standardů.

- **Cloud Security Alliance Open Certification Framework**

„Cloud Security Alliance Open Certification Framework" (dále jen CSA OCF) je certifikační rámec, za jehož vývojem stojí CSA.

CSA je mezinárodní nezisková organizace zabývající se především bezpečnostními otázkami cloud computingu. V této oblasti se věnuje výzkumu, poradenství, školení a dalším činnostem. V rámci CSA funguje více než 20 pracovních skupin, které maji jednotlivé činnosti na starosti.

CSA OCF poskytuje tři úrovně certifikací, jež spadají pod příslušné STAR programy („Security, Trust and Assurance Registry", tedy Registr bezpečnosti, důvěry a jistoty). Certifikace je možno získat třemi způsoby:

- Sebehodnocením poskytovatelů.
- Audit provedený třetí stranou.
- Kontinuálním monitoringem služeb

S tím, že poslední způsob je stále ve vývoji. První způsob umožňuje získání nejnižšího certifikačního stupně „**STAR Self-Assessment**". Nejedná se však o přihlášení se k nějakým principům, ale poskytovatelé musí podat report dokumentující dodržování bezpečnostních požadavků CSA (stanovených v dokumentu „CSA Cloud Controls Matrix"), případně zodpovězením a zasláním podrobného dotazníku.

Druhým způsobem lze získat certifikaci „**STAR Attestation**" a „**STAR Certification**", které mohou udělit certifikační orgány akreditovány CSA. Obě certifikace potvrzují kompatibilitu s CSA Cloud Controls Matrix, s tím, že první k tomu přidává kompatibilitu s americkým standardem SOC-2 (Service Organization Controls) a druhý s normou ISO/IEC 27001.

CSA na svých stránkách poskytuje seznam všech certifikovaných poskytovatelů/služeb včetně základních informací o službě, datu udělení certifikátu atd. Certifikovaných poskytovatelů/služeb je v současnosti více než 100. **Momentálně se jedná o nejrozšířenější certifikační schéma zaměřené výhradně na cloudové služby.** Jistou jeho slabinou však je, že se zaměřuje pouze na bezpečnostní otázky cloud computingových služeb a jiné aspekty nechává zcela bez povšimnutí.

- **EuroCloud Star Audit**

Certifikační schéma EuroCloud Star Audit bylo vyvinuto evropskou neziskovou organizací EuroCloud Europe založenou v roce 2009 a nyní zastoupenou v 21 zemích Evropy (ČR chybí).

Certifikace je rozdělena na pět stupňů, z nichž nejnižší (1 hvězda) vyžaduje splnění nejmenšího počtu požadavků (např. služba musí umožňovat smazání dat po ukončení právního vztahu). Nejvyšší stupeň (5 hvězd) stanovuje požadavky například i na rozložení datových center, na kterých je certifikovaná služba provozována [EUROCLOUD, © 2010 – 2015].

Certifikace je možná pouze akreditovanými zástupci organizace EuroCloud Europe. **Výhodou** tohoto certifikačního schématu je velké **zastoupení hodnocených oblastí,** ne tedy pouze bezpečnosti jako u předchozích certikačních schémat, ale také oblasti smluv, zákaznické podpory, interoperability, finanční situace provozovatele a další. Největší nevýhodou je tedy malé rozšíření. V současnosti je takto certifikováno teprve cca 10 služeb.

2.6. Legislativní okruh PESTL analýzy

Organizace veřejného sektoru se při přechodu ke cloudovým službám a jejich využívání musí vyrovnat s některými legislativními otázkami a požadavky. Ty lze rozdělit do dvou základních skupin [HELLEMANS, 2014]. První jsou obecné otázky týkající se např. rozhodného práva, ochrany osobních dat či smluvního rámce mezi poskytovateli a uživateli cloudu. Druhou jsou pak otázky specifické pro veřejný sektor jako např. zákon o veřejných zakázkách, případně otázky výhradní pro některé sektory jako jsou zdravotnictví či

bezpečnostní složky státu. V této kapitole se budeme věnovat první skupině a ve stručnosti představíme českou legislativu relevantní pro cloud computing.

2.6.1. Česká legislativa

Stejně jako v ČR neexistuje žádná státní strategie zaměřená na využívání cloud computingu, tak neexistuje žádná legislativa zabývající se přímo cloud computingem. Taková legislativa samozřejmě není nutná, a jak bylo zmíněno výše, ani se neplánuje, stejně tak jako žádná další legislativa specifická pouze pro určité technologie.

Právní rámec pro využívání cloud computingu je dán již existujícími zákony. Z pohledu organizací veřejného sektoru se při používání cloudových služeb jedná především o tyto zákony:

- **Zákon č. 101/2000 Sb., o ochraně osobních údajů**

  Vlivu tohoto zákona na využití služeb veřejného cloudu se budeme blíže věnovat v rámci samostatné podkapitoly VIZ KAP

- **Zákon č. 365/2000 Sb., o informačních systémech veřejné správy**

  Zákon stanovující práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. Tedy i systémů provozovaných „v cloudu". Využití veřejného cloudu pro provoz informačního systému veřejné správy zákon nezakazuje, ale přímo dovoluje. Jak stojí v § 2 písmene d): Provozováním informačního systému veřejné správy může správce (informačního systému) pověřit jiné subjekty, pokud to jiný zákon nevylučuje.

- **Zákon č. 227/2000 Sb., zákon o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)**

  Tento zákon upravuje v souladu s právem Evropských společenství používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky. Z pohledu cloudových služeb se tedy jedná především o zajištění důvěrnosti přenášených dat a autentizaci uživatelů.

- **Zákon č. 137/2006 Sb., o veřejných zakázkách**

  Vlivu tohoto zákona na využití cloudových služeb je věnován samostatný oddíl níže v textu.

- **Zákon č. 106/1999 Sb., o svobodném přístupu k informacím**

  Veřejné instituce mají povinnost dle tohoto zákona poskytovat informace zaznamenané na jakémkoliv nosiči, tedy i informace uložené v cloudu. Je tedy nezbytné, aby byla zajištěna včasná dostupnost všech informací uložených v cloudu a nic nebránilo jejich poskytnutí dle tohoto zákona.

- **Zákon č. 499/2004 Sb., o archivnictví a spisové službě (vč. vyhlášky 646/2004 Sb., o podrobnostech výkonu spisové služby)**

  Instituce, jež mají povinnost vykonávat spisovou službu, která je tímto zákonem definována jako „zajištění odborné správy dokumentů vzniklých z činnosti původce, ... , zahrnující jejich řádný příjem, evidenci, ... , oběh, .., odesílání, ukládání ...” by měly zajistit její naplňovaní v souladu se zákonem i v prostředí cloudových služeb.

- **Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti**

  Využití služeb veřejného cloudu pro práci s utajovanými informacemi spadajících pod tento zákon se prakticky vylučuje. Informační systém nakládající s utajovanými informacemi musí být schválen Národním bezpečnostním úřadem, který při certifikaci postupuje dle předpisu č. 523/2005[23]. Dle § 9 tohoto předpisu v zásadě ani nedovoluje připojení takových systémů do veřejné sítě. Zákon sice povoluje výjimky, ale je třeba získání patřičných oprávnění, jež bude pro poskytovatele veřejných cloudových služeb patrně příliš náročné a ekonomicky neefektivní. Je třeba přiznat, že toto je pouze autorova domněnka.

- **Zákon č. 563/1991 Sb., o účetnictví (včetně prováděcích vyhlášek)**

  Cloudové služby jsou poptávány, dle zákona č. 137/2006 Sb, o veřejných zakázkách, jako veřejné zakázky na služby. Náklady uživatele v tomto případě nejsou tedy investiční, ale provozní. To, jak tvrdí [PETERKA, 2012a], má bezprostřední důsledky jak pro plánování těchto nákladů, tak i v oblasti účetnictví, jež je pokryta tímto zákonem.

- **Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon)**

  Autorský zákon upravuje licenční podmínky, dle § 46 tedy oprávnění k výkonu práva dílo (jímž může být i počítačový program) užít, jež se uplatňují především při využívání cloudových služeb modelu SaaS.

[23] Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor

- **Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen ZKB)**

  ZKB má být řešením problematiky ochrany kyberprostoru vedoucí k zajištění kybernetické bezpečnosti státu. Zavádí povinnost implementovat řídící systém bezpečnosti informací a stanovit bezpečnostní politiku pro veřejné instituce, které plní buď roli „správce informačního systému kritické informační infrastruktury" anebo roli „správce významného informačního systému", případně poskytovatele služeb, jež tyto systémy provozují. Informační systémy kritické informační infrastruktury a významné informační systémy jsou určeny vyhláškou č. 317/2014, o významných informačních systémech a jejich určujících kritérií. Zákon do velké míry kopíruje požadavky na bezpečnost dle norem ISO 27001 a 27002.

2.6.2. Právní závazky ochrany osobních údajů v cloudu

Jak upozorňuje Úřad pro ochranu osobních údajů (dále jen ÚOOÚ), při provozování cloudových služeb je pravděpodobné, že dojde k práci s osobními či citlivými údaji [PAVLÁT, 2013]. Práva a povinnosti při zpracování osobních údajů jsou stanovena v zákoně č. 101/2000 sb., o ochraně osobních údajů a o změně některých zákonů (dále jen ZOOÚ). Zákon také stanovuje podmínky, za nichž se uskutečňuje předání těchto údajů do jiných států (tedy do států Evropské unie a tzv. třetích zemích), což je situace, která při využívání cloudových služeb může vzhledem k jejich povaze nastat. ZOOÚ vychází z evropské směrnice 95/46/ES.

Nejprve vymezíme základní pojmy stanovené ZOOÚ, kterými jsou osobní a citlivý údaj, a dále základní role (zpracovatel a správce), do kterých se subjekty nakládající s těmito údaji mohou dostat a co se myslí zpracováním údajů.

Osobní údaj - *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu."*

Citlivý údaj - „osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů."

Správce - „každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak."

Zpracovatel - každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.

Zpracování osobních údajů - jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

Osobní údaj je definován poměrně široce, ale to má svůj význam. Třeba IP adresa sama o sobě není nutně osobním údajem, ale stává se jím v určitém kontextu nebo ve spojení s jinými údaji. Některé údaje jako jméno, rodné číslo či číslo platební karty jsou osobními údaji vždy.

V rámci vztahu mezi uživatelem a poskytovatelem cloudové služby obvykle[24] vystupuje **uživatel jako správce**[25] a **poskytovatel jako zpracovatel**. Uživatel cloudových služeb určuje konečný účel zpracování a rozhoduje o zadání tohoto zpracování nebo jeho části externí organizaci [EVROPSKÁ KOMISE, 2012b]. Pro uživatele cloudu z toho vyplývá, že je zodpovědný za dodržování právních předpisů a vztahují se na něj všechny právní závazky stanovené ZOOÚ. Uživatelovou povinností je vybrat si takového poskytovatele cloudových služeb, který zaručuje soulad s právními předpisy.

Cloudové služby jsou často poskytovány ve standardizované formě a uživatel prakticky nemá šanci vyjednat individuální smluvní podmínky, ale ani tato nerovnováha, s ohledem na smluvní sílu malého správce údajů vůči poskytovatelům služeb, jak upozorňuje [EVROPSKÁ KOMISE, 2012b], by se neměla považovat za důvod, aby správce přijal ustanovení a podmínky smlouvy, jež není v souladu s právem v oblasti ochrany údajů.

[24] Může dojít i k situaci, kdy poskytovatel cloudu vystupuje jako správce (např. když zpracovává údaje pro svou potřebu) [EVROPSKÁ KOMISE, 2012b].

[25] Myšleno pro případy, kdy jako uživatel vystupuje nějaká instituce, resp. právnická osoba. Pokud je uživatelem fyzická osoba, využívající služby výhradně k osobním či domácím aktivitám, může zde platit tzv. vyjímka pro domácí použití, podle níž uživatelé správce nepředstavují (stanovisko 05/2012 WP29).

2.6.3. Předávání osobních údajů do jiných států

Jak již bylo zmíněno, k předávání osobních údajů do jiných států může, a často se tak i děje, v rámci využívání cloudových služeb docházet. V některých případech je třeba, aby správce (uživatel) přijal dodatečně zvláštní záruky pro přenos údajů.

Zvláštních záruk není třeba v případě, že údaje jsou uchovávány a zpracovávány v zemích EU, kde je volný pohyb osobních údajů zaručen směrnicí 95/46/ES a z ní vyplývajících zákonů jednotlivých států. Stejné podmínky platí pro země, které ratifikovaly Úmluvu 108 a pro země, o kterých Komise EU rozhodla, že poskytují přiměřenou úroveň ochrany[26].

V případě, že osobní data budou zpracovávána v zemi, která nesplňuje žádná z výše uvedených kritérií, je správce (uživatel) povinnen zajistit, že datům bude poskytnuta odpovídající ochrana. K tomu se využívá **standardních smluvních doložek**, **závazná podniková pravidla** či institut **Safe Harbor** (pro zpracovávání na území USA).

Standardní smluvní doložky, jejichž vzorové verze jsou přílohou rozhodnutí Komise 2010/87/EU, slouží ke snadnějšímu předávání osobních údajů správcem údajů sídlicím v EU zpracovateli usazenému ve třetí zemi [EVROPSKÁ KOMISE, 2010]. Výhodou těchto smluvních doložek je, že pokud se stanou součástí smlouvy o poskytování cloudových služeb, není třeba žádat Úřad pro ochranu osobních údajů o speciální povolení pro vydávání údajů.

Závazná podniková pravidla (Binding Corporate Rules, dále BCR) jsou poměrně novým právním instrumentem. Jedná se o interní pravidla pro nadnárodní korporace, jejichž některé části mohou sídlit i mimo EU, zavazující je poskytnout adekvátní ochranu při zpracovávání osobních dat, tak jak je požadováno směrnicí 95/46/ES [EUROPEAN COMMISSION, 2014]. BCR korporace musejí projít schvalovacím řízením alespoň 3 členských států EU, což může být zdlouhavá procedura, ale po jejich získání již není třeba vytváření nějakých ad hoc smluvních doložek.

Dalším speciálním instrumentem, který lze využít pro předávání citlivých údajů je rámec označovaný jako **„Safe Harbor"** (Bezpečný přístav). Ten umožňuje volné předávání osobních údajů správci v zemích EU zpracovatelům sídlícím v USA, které jsou jinak považovány z legislativního hlediska za zemi s nedostatečnou ochranou osobních údajů.

[26] Seznam těchto zemí je dostupný z http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=8&DF=&CL=ENG.

Na základě rozhodnutí Komise EU z roku 2000 bylo uznáno, že zásady „Safe Harbor" a „Frequently Asked Questions" (často kladené otázky, dále FAQ), vydané Ministerstvem obchodu USA, poskytují adekvátní ochranu pro přenosy osobních údajů z EU do USA.

Správci (uživatelé) mohou předávat osobní údaje organizacím v USA, které přijaly 7 zásad „Safe Harbor" (např. zajištění dostačující ochrany proti ztrátě dat) a 15 FAQ. Přihlášení se k těmto zásadám je dobrovolné. Organizace to musí oznámit ve svých veřejně dostupných pravidlech ochrany soukromí a nahlásit se Ministerstvu obchodu USA. V současnosti je takovýchto organizací více než 3000.

Institut „Safe Harbor" v poslední době čelil značné kritice a nejistotě o jeho dalším fungování. Kromě velkého nárůstu účastníků (v roce 2004 bylo přihlášeno pouze 400 organizací), jež může znesnadnit sledování toho, jak jsou zásady skutečně splňovány, se jedná především o obavy způsobené (viz např. [KROES, 2013]) odhalením rozsahu porušování práva na soukromí Národní bezpečnostní agenturou USA[27].

K institutu „Safe Harbor" je dále také třeba dodat, že je na správci (uživateli), aby si ověřil, že případný poskytovatel cloudových služeb se skutečně nachází na seznamu schválených organizací. Dle zprávy Evropské komise (2013b) až 10% organizací hlásících se k „Safe Harbor" ve skutečnosti na seznamu Ministerstva obchodu USA není.

Využití poskytovatele cloudových služeb, jehož jediná záruka nakládání s osobními daty dle platné evropské legislativy je přihlášení se k zásadám Safe Harbor, je z právního pohledu v pořádku, ale přesto lze doporučit důsledné zhodnocení uživatelem, zda je taková ochrana dostačující. Při jakýchkoliv pochybách by mělo být přistoupeno k použití standardních smluvních doložek, které by měly být spolehlivějším a hlavně vymahatelnějším závazkem. Závazná podniková pravidla se v tomto ohledu zdají mnohem spolehlivějším ukazatelem skutečného naplňování podmínek EU pro zacházení s osobními a citlivými údaji, ale jejich akceptace se dá očekávat pouze u největších mezinárodních poskytovatelů cloudových služeb.

2.6.4. Rozhodné právo

Rozhodné právo určuje legislativu státu, která bude výchozí pro tvorbu samotné smlouvy jako pro řešení případných sporů vzniklých mezi poskytovatelem a uživatelem.

Pokud není uzavřená písemná smlouva, která jasně stanovuje rozhodné právo a vychází se ze standardních smluv poskytovatele cloudových služeb, pak je obvykle rozhodné právo dáno

[27] více info např. zde
http://en.wikipedia.org/wiki/Global_surveillance_disclosures_%282013%E2%80%93present%29

státem, ve kterém má poskytovatel své hlavní sídlo, případně tím, v jaké zemi poskytuje nejvíce služeb [BRADSHAW, 2010]. S tím mohou vznikat různé překážky pro bezproblémové využívání cloudových služeb.

Pro instituce veřejného sektoru se v případě vypisování výběrového řízení jeví jako nejlepší řešení zmínit požadavek na rozhodné právo již v zadávací dokumentaci výběrového řízení (vysvětleno v následujícím oddíle).

2.6.5. Poptávání cloudových služeb

Instituce veřejného sektoru poptávající veřejné cloudové služby (zadavatel) musí postupovat dle zákona č. 137/2006 Sb., o veřejných zakázkách (dále jako ZVZ). V tomto případě jde o veřejné zákázky na služby dle ZVZ.

Zadavatel musí vytvořit zadávací dokumentaci, která vymezuje předmět zakázky a stanovuje předpokládanou hodnotu zakázky. Součástí dokumentace musí být dále obchodní podmínky (platební podmínky, doba trvání služby, stanovení rozhodného práva apod.), technické parametry a další požadavky dle § 44 ZVZ. V rámci kvalifikačních požadavků na uchazeče lze také stanovit certifikace, kterými by měl uchazeč o zakázku disponovat. Jak vyplývá z rozboru certifikačních schémat v předchozí podkapitole, tak prakticky jedinou certifikací, která v současnosti připadá v úvahu (alespoň v oblasti bezpečnosti) je certifikace dle normy ISO 27001, případně CSA Star Audit.

Nejasné nebo nedostatečně specifické zadání veřejné zakázky může vést k obdržení neporovnatelných nabídek. To může mít za následek až zrušení veřejné zakázky, případně vést, jak varuje Peterka [2012a], *„k „vysoutěžení“ veřejné zakázky, která neodpovídá představám, resp. potřebám zadavatele*“. To v konečném důsledku může být ještě horší varianta než zrušení zadávacího řízení.

Z hlediska stanovení technických parametrů se autorovi jeví obtížné především poptávání cloudových služeb v podobě servisního modelu IaaS. V zadávací dokumentaci je třeba popsat velice konkrétně požadavky na technické parametry poptávaných výpočetních zdrojů (výkon procesorů, kapacita datových úložišť, datová propustnost síťových prvků apod.). Zde může docházet k jisté limitaci využitelnosti škálovatelného charakteru cloudových služeb. Ten je totiž limitován povinností stanovit předpokládanou hodnotu zakázky, jež může být v případě využití IaaS velice těžko vypočitatelná.

Poptávání cloudových služeb modelu SaaS se jeví z technického hlediska o něco jednodušší. Požadavky na zadávací dokumentaci pro SaaS popisuje Pattynová [2012], dle které musí

obsahovat předmět zakázky, tedy jasně definovat parametry požadované služby, dobu trvání služby, počet (alespoň rámcově) a kategorie uživatelů služby (někteří mohou mít přístup pouze k některým službám), časový interval, po kterém se mohou měnit počty uživatelů (např. po půl roce), a dále požadavky na zabezpečení dat a případně požadavek na stanovení rozhodného práva.

Dalším důležitým krokem je výběr zadávacího řízení. V případě cloudových služeb připadají v úvahu 3 způsoby, a to otevřené řízení, rámcová smlouva či dynamický nákupní systém.

Jako nejvhodnější se jeví využití rámcové smlouvy, která nejlépe umožňuje zachovat výhody plynoucí ze škálovatelnosti cloudových služeb [PATTYNOVÁ, 2012]. § 11 ZVZ definuje rámcovou smlouvu jako smlouvu uzavřenou na dobu určitou, upravující podmínky mezi jedním nebo více dodavateli týkajících se opakujícího se poskytnutí služby. Zadavatel tak uzavře rámcovou smlouvu s dodavatelem, na jejímž základě bude probíhat např. nákup licencí na SaaS. Stanovení předpokládané ceny za zakázku je u rámcové smlouvy maximální předpokládaná hodnota všech zadaných veřejných zakázek v době trvání rámcové smlouvy. U SaaS se to tedy dá např. stanovit vynásobením maximálního počtu uživatelů předpokládanou cenou za jednoho uživatele. Model SaaS je také obvykle poskytován v předplatitelském platebním modelu, který výpočet předpokládané ceny ulehčuje [PATTYNOVÁ, 2012].

2.6.6. Smluvní vztah mezi poskytovatelem a uživatelem

Při využívání cloud computingových služeb spolu poskytovatel a uživatel vstupují do právního vztahu, který by měl být ideálně ošetřen písemnou smlouvou. V případě smluvního vztahu vzniklého na základě veřejné zakázky to je dokonce nutnost.

Druhá možnost spočívá ve využití neplacených služeb, na které se nevztahuje povinnost vyhlášení výběrového řízení. Jedná se především o některé produkty modelu SaaS. Ty mají smluvní podmínky dané a jejich individuální úprava není možná.

V případě placených služeb může být prostor pro vyjednání individuálních podmínek. Ne vždy to je však možné. Záleží také na velikosti instituce a tím její vyjednávací síle. Čím větší instituce, tím větší zákazník (respektive zakázka), u kterého se dá předpokládat, že poskytovatelé cloudových služeb, často velké mezinárodní společnosti, budou ochotní přistoupit na individuální smlouvu.

Důležité je nezapomenout, že povinností uživatele je přistoupit pouze na takové podmínky, které nebudou v rozporu s platnou legislativou a to především s ohledem na již zmíněné

aspekty. Dobře nastavené smluvní podmínky, jak upozorňuje ICTU, jsou základem toho, aby využívání cloudových služeb naplnilo očekávání [PETERKA, 2012a].

Smluvním vztahům mezi poskytovateli a uživateli cloudových služeb se věnuje celá řada studií (např. [JISC, 2011], [Černý, 2014], [PATTYNOVÁ, 2012]) ze kterých lze vyvodit rámcová doporučení pro smluvní vztah mezi uživatelem a poskytovatelem služby. Následující doporučení se týkají především situace, kdy je uživatel v pozici, ve které si může vyjednat individuální smlouvu. V případě standardizovaných smluv je především třeba provést analýzu, zda jejich akceptace a následné využívání služby nebude v rozporu se zákonem.

Smlouva by měla jasně **definovat poskytovanou službu** včetně časového rozvrhu služby. Součástí smluvního vztahu bývá obvykle samostatná **smlouva o úrovni poskytovaných služeb** (service-level agreement, dále jen SLA), která garantuje dostupnost a kvalitu služby. Garantovaná dostupnost služby je obvykle uváděna v procentech (např. 98 % nebo 99%) doby, po kterou je služba dostupná. Tomu je třeba věnovat patřičnou pozornost, neboť celkový čas, kdy služba nemusí být dostupná, je velice rozdílný (viz následující tabulka). SLA by měla také stanovit sankce za porušení jejího plnění (např. v podobě slevy či zrušení poplatku za dobu, kdy nebyla dostupná) a objektivní měřící techniky pro sledování jejího plnění.

Dostupnost	roční nedostupnost	měsíční nedostupnost
98 %	7.3 dnů	14,4 hodin
99 %	3,65 dnů	7,20 hodin
99, 8 %	17,52 hodin	86,26 minut
99, 9 %	8,76 hodin	43,8 minut

V první řadě by měla vzniknout **migrační smlouva**, která ošetřuje přechod na cloudovou platformu. Popis nejdůležitějších oblastí, které by měly být součástí migrační smlouvy udává Jansa (2012): vytvoření zálohy dat pro případ, že by během migrace došlo k jejich ztrátě; plán migrace v podobě harmonogramu veškerých činností nutných pro migraci dat; přesnou definici stávajícího a cílového migračního prostředí; předmět migrace v podobě závazků zúčastněných stran na spolupráci a stanovení ceny za migraci a stanovení sankcí za případné porušení.

Ošetřit je třeba také postup při ukončení smlouvy mezi poskytovatelem a uživatelem. Tento plán bývá označován jako „**exit strategie**". Jedná se v podstatě o migrační smlouvu naruby. Exit strategie by měla být vyřešena ještě před migrací na cloudové řešení, protože, jak upozorňuje [PETERKA, 2012a], součinnost poskytovatele při „exitu" nemusí být zdaleka tak samozřejmá a automatická jako při „vstupu". Kromě postupu převedení dat ven z cloudu je vhodné také zajistit, aby poskytovatel data smazal ze svých serverů. Správně nastavená exit strategie je také jednou z podmínek vyhnutí se závislosti na jediném dodavateli (tzv. vendor „lock-in").

Migrační smlouva a exit strategie popisují přechod ke cloudovým službám a jejich opouštění. Další důležitou oblastí, která by v rámci smluvního vztahu měla být pokryta, jsou **data uživatele** a to nejen osobních a citlivých údajů, jejichž nutnosti zakotvení ve smlouvě byl věnován předchozí oddíl. Smluvně by se mělo také ošetřit **zacházení s daty** v době, kdy se budou nacházet v cloudovém prostředí. Poskytovatel by měl poskytnout obecné bezpečnostní záruky o zajištění ochrany uživatelových dat. Další oblastí, která by v rámci zacházení s daty měla být smluvně pokryta je přístup poskytovatele k datům. Kromě obecného závazku o důvěrnosti dat by zaměstnanci poskytovatele, kteří se k datům mohou dostat, měli být vázáni dohodou o mlčenlivosti. Součástí smluvního vztahu by mělo být také ujištění, že data, i když jsou umístěna v infrastruktuře poskytovatele, stále patří uživateli.

Černý [2014] varuje před vágními formulacemi, které se mohou vyskytovat zejména ve standardizovaných podmínkách poskytovatele, umožňující využívat data uložená v cloudu v prospěch poskytovatele (data mining). Takovými formulacemi mohou být např. „k ochraně našich (poskytovatelových) zájmů" či „k poskytování cíleného obsahu".

Poskytovatel by měl být vázán k poskytnutí informací o bezpečnostních incidentech (únik, ztráta či poškození dat) a také o případných žádostech státních orgánů (i cizích států) o přístup k uživatelovým datům.

V rámci smluvního vztahu by mělo být také ošetřeno **rozhodné právo**, tedy legislativa jakého státu bude použita pro řešení případného soudního sporu. Zde lze jednoznačně doporučit vyhledání takového poskytovatele, který je schopen zaručit řešení sporu dle právního řádu ČR.

Dosud byly zmiňovány především povinnosti, ke kterým by měl být zavázán poskytovatel cloudových služeb. Povinnosti však vznikají i na straně uživatele. Poskytovatelé se především chrání před zneužitím svých služeb pro nelegální činnost případně proti takovému využití služeb, které by mohlo ohrozit jejich funkčnost či poškodit jiné uživatele služby.

Problematika smluvního vztahu mezi uživatelem a poskytovatelem byla popsána stručně a rámcově, tak aby přinesla základní vhled do této problematiky. V reálných případech uzavírání smluvního vztahu mezi poskytovatelem a uživatelem z veřejného sektoru je nutné brát v potaz i další faktory, jako vnitřní pravidla organizace. Do smluvního vztahu často také vstupují další subjekty, jako subdodavatelé poskytovatele služeb, jejichž vliv je třeba také právně ošetřit (nejlépe jasnou odpovědností poskytovatele). Každý případ musí být posuzován individuálně, nejlépe právní expertízou s ohledem na velikost a kritičnost zvažovaných cloudových služeb.

3. SWOT analýza

3.1. Definice SWOT analýzy

SWOT analýza je analytickou technikou pro pro zhodnocení vnitřních (silné a slabé stránky) a vnějších (příležitosti a hrozby) faktorů analyzovaného subjektu, kterým může být např. nějaká organizace, technologie či projekt [MANAGEMENTMANIA.COM, 2013b].

SWOT analýza vznikla na půdě amerického Stanfordského výzkumného ústavu v 60. a 70. letech 20. století během práce analytického týmu pod vedením Alberta Humphreyho na anlaýze firem, které se dostaly na žebříček „Fortune 500" (žebříček firem v USA s největším obratem) [FRIESNER, 2014].

3.2. Metodický postup analýzy

Vzhledem k tomu, že metoda SWOT analýzy nepodléhá žádné standardizaci, je třeba vysvětlit metodický postup provedené analýzy. Analýza byla provedena na základě studia dostupných materiálů a aplikací zjištěných faktů na prostředí a možnosti využití služeb cloud computingu v prostředí českého veřejného sektoru.

Silné a slabé stránky představují vnitřní prostředí cloud computingu. Silné stránky vycházejí z definice a vlastností cloudových služeb a zároveň představují výhody cloud computingu a to především vůči tradičnímu způsobu přístupu k ICT technologiím, které jsou plně ve správě uživatele („on-site"). Slabé stránky naopak popisují nevýhody plynoucí z využívání cloudových služeb. Silné a slabé stránky vyplývají ze samotné podstaty cloud computingu a zároveň z nich plynou příležitosti (v případě silných stránek) a hrozby (v případě slabých stránek). Příležitosti a hrozby vycházejí z vnitřního prostředí (silné a slabé stránky) a zároveň jsou ovlivňovány a naopak samy mohou ovlivnit vnější prostředí, jež bylo popsáno v rámci PESTL analýz. Výsledkem analýzy jsou konkrétní faktory, stručně vypsané v tabulce (viz níže) s odkazy na jejich detailnější popis dále v textu.

3.3. Tabulka faktorů SWOT analýzy

Kap.	Silné stránky	Kap.	Slabé stránky
3.4.1	Sdílení prostředků	3.5.1	Závislot na Internetu
3.4.2	Jednoduchost používání	3.5.2	Chybějící jazykové lokalizace
3.4.3	Flexibilita a rychlost nasazení	3.5.3	Nepřehlednost trhu
3.4.4	Energetická úspornost	3.5.4	Nedostatěčná standardizace
3.4.5	Dostupnost a přístupnost	3.5.5	Financování skrze EU fondy
3.4.6	Automatická aktualizace		
3.4.7	Centralizované zabezpečení		
3.4.8	Obnova dat po havárii		
3.4.9	Měřitelnost služeb		
Kap.	**Příležitosti**	**Kap.**	**Hrozby**
3.6.1	Finanční úspory	3.7.1	Bezpečnostní rizika
3.6.2	Lepší využití ICT odborníků	3.7.2	„Vendor lock-in”
3.6.3	Zvýšení přistupnosti	3.7.3	Nedostatečná připravenost
3.6.4	Jednodušší spolupráce	3.7.4	Chybějící zkušenosti
		3.7.5	Nepřehledná politcká situace
		3.7.6	Špatné smluvní podmínky
		3.7.7	Kulturní bariéry v organizaci

3.4. Silné stránky

3.4.1. Sdílení prostředků

Sdílení prostředků je vlastností, která stojí za často udávanou ekonomickou výhodností cloudových řešení. Datová centra velkých poskytovatelů cloudových služeb dokáží těžit z tzv. „úspor z rozsahu" (economies of scale) a to především ve třech oblastech:

- Dosažení úspor na straně dodávek vybavení a energií.
- Sdružování poptávky.
- Multi-tenant architektura [ETRO, 2011].

Poskytovatelé mohou dosáhnout úspor na straně dodávek HW vybavení, vzhledem k tomu, že mohou nepochybně získat výhodnější cenové podmínky při nákupu HW vybavení pro vybudování svých datových center.

Další oblastí, kde se poskytovatelé snaží ušetřit, jsou náklady na energetické zdroje, především tedy elektrickou energii. Datová centra jsou tak budována v zemích s nízkou cenou elektrické energie, jako jsou např. skandinávské země [VERGE, 2014], jež používají ve velké míře obnovitelné zdroje. A díky klimatickým podmínkám v těchto zemích nejsou tak velké nároky na chlazení data center, čímž vznikají další úspory.

Energetická úspornost cloudových služeb dává příležitost nejen pro finanční úspory, ale také ke snižování negativního dopadu ICT služeb na životní prostředí.

Sdružováním poptávky, tedy hostováním služeb pro široký segment zákazníků, je možné docílit vysoké utilizace kapacity datových center. Utilizace v klasických datových centrech je obecně nízká. Rozmezí utilizace se udává v rozpětí 10 - 20 % (Vivek Kundra, již zmíněný autor americké FCCI, reportoval utilizaci amerických vládních serverů na úrovni pouhých 7 % [MILLER, 2010]), což není mnoho. Data centra, poskytující veřejné cloudové služby, dokáží utilizaci zvýšit díky široké uživatelské bázi. Široká báze zde není jen ve smyslu velkého počtu, ale také ve smyslu geografického rozšíření, oborové rozmanitosti atd. Díky těmto faktorům se rozloží jednotlivé špičky ve využívání zdrojů a nedochází tak k dlouhým obdobím, kdy nejsou servery využívané. K větší utilizaci samozřejmě také pomáhá virtualizační techniky a automatizace datových center (jež byly popsány úvodní kapitole).

Multi-tenant architektura aplikací slouží k zpřístupnění jedné služby (instance), která běží na jediném fyzickém (či virtuálním) serveru, více zákazníkům (tenant). Využití multi-tenant architektury opět vede k lepší utilizaci zdrojů a tím i menší ceně za služby pro uživatele.

3.4.2. Jednoduchost používání

Cloudové služby jsou obvykle vytvářeny se záměrem uživatelské přívětivosti. Služby servisního modelu SaaS jsou z uživatelského hlediska stejné jako jejich desktopové verze.

Aspekt jednoduchosti používání nelze omezit jen na koncové uživatele a na model SaaS. Správa ICT zdrojů v cloudu (včetně IaaS i PaaS modelů) probíhá pomocí webového rozhraní, jež usnadňuje práci i správcům informačních technologií organizace.

3.4.3. Flexibilita a rychlost nasazení

Flexibilita cloudových služeb je dána jejich vysokou pružností, škálovatelností a samo obslužností. Lze tak jednoduše a hlavně velmi rychle přidávat či odebírat zdroje a to na základě aktuální potřeby. To opět směřuje k finanční výhodnosti cloudových služeb oproti klasickému „on-site" řešení.

V případě využívání modelu IaaS uživatel tedy nepotřebuje mít ve vlastnictví servery s výpočetní kapacitou nutnou ke zvládnutí provozní špičky, která může v některých případech nastat třeba jen několikrát do roka při zvláštních událostech (např. zápis předmětů na začátku akademického roku, poslední dny při odevzdávání daňových přiznání atd.).

V případě SaaS odpadá nutnost instalace aplikací na jednotlivá koncová zařízení. Zároveň lze jednoduše přidávat a odebírat uživatele (resp. dokupovat oprávnění pro využívání služeb nebo naopak odhlašovat).

Doba nasazení cloudových služeb se obecně udává jako nižší oproti klasickým ICT řešením. To je z charakteru cloudových služeb pochopitelné, ale velmi záleží na komplexnosti nasazovaného řešení, jak vyplývá ze zkušeností popsaných v poslední kapitole této práce.

3.4.4. Energetická úspornost (Green ICT)

V tradičně pojatém IT zázemí je obvykle potřeba velkých data center neustále vyžadujících elektrickou energii k provozu a chlazení. Přechodem ke cloudovým službám odpadá potřeba vlastnit a spravovat velké množství výpočetních technologií, v závislosti na tom, kolik a jakých zdrojů je do cloudu přemístěno. Tím klesá spotřeba energií na straně uživatele. Naopak, na straně druhé, u poskytovatelů nedochází tolik k zbytečnému plýtvání s energiemi, jak bylo popsáno výše v textu.

Díky větší utilizaci cloudových data center (viz bod „ekonomická výhodnost") cloudové technologie často nesou označení „Green ICT" a jsou považovány za ekologicky šetrnější oproti klasickému IT.

3.4.5. Velká přístupnost a dostupnost cloudových služeb

Data či aplikace umístěné v cloudu jsou přístupné z jakéhokoliv místa s připojením k Internetu. Přístupnost je zde dána nezávislostí na koncovém zařízení uživatele. Uživatelé nejsou limitováni zařízením, které pro přístup ke cloudu používají (i když je zde jistá limitace např. v požadavcích na verze webových prohlížečů). Ke komunikaci mezi uživatelem a cloudovou službou dochází na webových rozhraních, jež jsou postavená na webových standardech a dokáží komunikovat s různými typy koncových zařízení bez ohledu na jejich typ, operační systém apod.

Dostupností je zde myšlena doba, po kterou jsou služby přístupné. Dostupnost, jak již bylo zmíněno v (VIZ KAP), by měla být řádně zakotvena v SLA. Obecně platí, že dostupnost služeb v cloud je vyšší než těch ve vlastní správě. Studie zkoumající dostupnost cloudových služeb 38 poskytovatelů uvádí, že průměrná dostupnost v roce 2014 byla 99,91 % [IWGCR, 2014].

3.4.6. Automatická aktualizace

Tím, že jsou výpočetní zdroje a aplikace (dle servisního modelu) na straně poskytovatele, odpadá uživateli starost se sledováním aktualizací a jejich následnou instalací.

Je však třeba zajistit, aby případné aktualizace softwaru, případně i zdrojů na nižší vrstvě, nezpůsobily problémy. U SaaS např. s dokumenty a soubory, které byly vyhotoveny pomocí starší verze. Je třeba ověřit, že poskytovatel služeb dává záruky zajištění kontinuality služeb.

3.4.7. Centralizované zabezpečení

Využívání cloudových služeb není bez rizika, jak ukazuje (VIZ KAP), ale na druhou stranu provoz služeb v cloudu je v mnoha ohledech bezpečnější. Poskytovatelé se pochopitelně snaží o co největší bezpečnost jimi nabízených služeb, k čemuž je vedou i čistě pragmatické důvody. Každý (odhalený) bezpečnostní incident je pro poskytovatele nepříjemný i z obchodního hlediska.

Report, zkoumající cílené útoky na webové aplikace provedený společností zabývající se bezpečnostní cloudových služeb Alert Logic, uvádí, že webové aplikace jsou napadány se stejnou měrou, ať už jsou provozovány v cloudu, či na serverech umístěných v data centru organizace. Rozdíl nastává v průniku, který je větší v druhém případě [COTY, 2012].

Poskytovatelé jsou schopni zajistit bezpečnost často na vyšší úrovni než je v možnostech jednotlivých uživatelů. Jak bylo popsáno v PESTL analýze (VIZ KAP), tak ICT odborníků je

ve veřejném sektoru nedostatek a využiti cloudových služeb přenáší velkou část odpovědnosti na poskytovatele, kteří musí zajistit patřičné zabezpečení.

3.4.8. Obnova dat po havárii

Většina cloudových služeb automaticky zálohuje data a to často přímo v reálném čase. Cloudová infrastruktura je také obvykle provozována v alespoň 2 geograficky oddělených lokalitách, takže by měla vydržet i náhlý výpadek jedné své části. Na rozdíl od klasického IT zázemí, jež je obvykle umístěno na jednom místě. Hrozba ztráty dat při havárii je tak podstatně menší v cloudovém prostředí.

3.4.9. Měřitelnost služeb

Měřitelnost je jednou ze základních vlastností cloudových služeb. V rámci služeb veřejného cloudu jsou měřící techniky využity především pro kalkulaci poplatků. Měřitelnost služeb však najde také využití při hodnocení skutečného používání služeb koncovými uživateli, ale také pro monitorování celkového zatížení výpočetních zdrojů uživatele. To může mít za následek i lepší pochopení ICT potřeb uživatele, jež lze využít pro další plánování rozvoje.

3.5. Slabé stránky

3.5.1. Závislot na Internetu

Hlavní podmínka využívání služeb veřejného cloudu je přípojení k Internetu. A zároveň to je také jedna z hlavních nevýhod. Ačkoliv, jak ukázala PESTL analýza, možnosti internetového připojení v ČR jsou na dobré úrovni, tak pro instituce veřejného sektoru v některých odlehlejších oblastech může být získání kvalitního připojení stále problém.

Cloudová služba může poskytovat vysokou míru dostupnosti, ale pokud tutéž míru dostupnosti negarantuje poskytovatel internetového připojení, tak to nemusí být příliš platné. Výpadky internetového připojení se do celkové dostupnosti cloudových služeb pochopitelně nezapočítávají.

V ideálním případě si uživatel zajistí záložní internetové připojení pro případy delších výpadků spojení, ale to se pak negativně projeví v celkových nákladech.

3.5.2. Chybějící jazykové lokalizace

Tato nevýhoda se vztahuje především k modelu SaaS, s jehož aplikacemi přicházejí do styku zaměstnanci instituce a případně i uživatelé z vnějšku, kteří musejí mít služby veřejného sektoru dostupné v úředním jazyce.

Aplikací SaaS je opravdu velké množství. Jenom v Digitálním tržišti Velké Británie, které je popsáno v PESTL analýze, je inzerováno 5159 služeb modelu SaaS, a to se jedná pouze o služby schválené pro využití institucemi veřejného sektoru. Naprostá většina z nich nemá českou lokalizaci, což je, vzhledem k tomu jak malý trh ČR a zvláště její veřejný sektor představují, pochopitelné. Zvláště pro menší poskytovatele SaaS se lokalizace patrně nevyplatí, zvláště pokud ani neexistuje nějaká státní podpora využívání služeb veřejného cloudu.

3.5.3. Malý a nepřehledný trh s cloudovými službami

Na začátek tohoto bodu je třeba objasnit, že je myšlen trh s lokalizovanými (případně přímo zde vytvořenými) službami, které může využit veřejný sektor. Pro srovnání s údaji o Digitálním tržišti ve Velké Británii, patrně nejkomplexnější webový portál v ČR poskytující přehled ICT služeb „SystemOnLine.cz" má v seznamu 69 řešení[28] v modelu SaaS - a zdaleka ne všechna řešení jsou určena či využitelná veřejným sektorem.

Trh s cloudovými službami je ze své podstaty globální a jednotlivcům nebo soukromým firmám nic nebrání v tom, aby plně využívaly jeho možností. Nutnost podstupovat výběrová řízení při akvizici placených služeb však veřejnému sektoru takovou volnost nedávají.

3.5.4. Nedostatečná standardizace

Ačkoliv práce na poli standardizace cloudových služeb probíhá opravdu hodně, jak bylo popsáno v PESTL analýze, stále chybí jasný konsenzus nad tím, jaké standardy by měly být v praxi využívány. To vede v praxi k omezení interoperability jednotlivých služeb a přenosnosti dat. Tento stav vede k tomu, že stále hrozí riziko uzamknutí se u jediného poskytovatele.

3.5.5. Financování skrze EU fondy

Možnosti financování pomocí fondů Evropské unie bylo popsáno v (VIZ KAP). Možnosti existují, ale pro financování služeb veřejného cloudu jsou značně limitovány. Vzhledem k podpoře cloud computingu v EU se jedná o situaci poněkud paradoxní.

3.6. Příležitosti

3.6.1. Finanční úspory

Předpoklad finančních úspor a celkové finanční výhodnosti cloud computingu vychází ze dvou hlavních předpokladů:

- **Přechod od CAPEX k OPEX**

[28] Údaje z Digitálního tržiště i webu SystemOnLine.cz byly získány 15. 4. 2015.

Kapitálové investice do pořízení ICT technologií představují velkou jednorázovou zátěž pro rozpočet a to zvláště institucí veřejného sektoru, které se musí v posledních letech potýkat se snižováním svých rozpočtů a limitací výdajů na ICT (VIZ KAP PESTL). Přechodem ke cloudovým službám je možné se právě těmto nákladům vyhnout a naopak přejít k nákladům provozním (OPEX). V cloudovém prostředí jsou tyto náklady účtovány na základě skutečné spotřeby (oceňované dle různých faktorů, jak je popsáno v rámci ekonomického okruhu PESTL analýzy).

To má za následek dvě veci. Za prvé, uživateli zůstanou k dispozici finanční prostředky, které by jinak musel investovat do požadovaného ICT vybavení a může je využít jinak [HARDING, 2011]. Za druhé, provozní náklady v cloudu mají lepší predikovatelnost, což platí dvojnásob u služeb, jež mají lineární charakter (jsou v průběhu času využívané stejně) či jsou placené paušálně (např. na základě počtu uživatelů) [PETERKA, 2012a]

- **Snížení TCO ICT infrastruktury**

Přechodem ke cloudovým službám se snižují celkové náklady vlastnictví (TCO) ICT infrastruktury uživatele (VIZ KAP), protože odpadají náklady spojené s údržbou a správou infrastruktury. A právě tyto náklady, dle průzkumu auditorské společnosti Deloitte [2014], představují až 82 % rozpočtu na IT ve veřejném sektoru. Z tohoto hlediska dávají cloudové služby institucím veřejného sektoru poměrně velký prostor pro úspory.

Jak bylo zmíněno v kapitole (VIZ KAP) popisující adopci cloudových služeb v USA, finanční úspory ne vždy představují hlavní motivaci pro jejich využití a ne vždy je možné úspor dosáhnout. Z tohoto pohledu představuje riziko především model SaaS. V průběhu času totiž cena zaplacená za užívání aplikací modelu SaaS dosáhne nebo převýší cenu, která by byla zaplacena přímou koupí softwaru. Avšak pokud je tohoto „vyrovnání" dosaženo během tří až čtyřletého období, tak bývá SaaS řešení považováno za výhodné [CREESE, 2011]. V případě SaaS jsou tedy hlavní výhodou jiné aspekty (např. automatické aktualizace, bezpečnostní řešení) zmíněné v rámci této SWOT analýzy. I přes to přechod k řešení na bázi SaaS snižuje TCO.

3.6.2. Lepší využití ICT odborníků

Odborníci na informační technologie jsou, jak popisuje kapitola (VIZ KAP), nedostatkové a drahé „zboží". Vzhledem k alokaci většiny rozpočtu na běžnou správu a údržbu ICT technologií je zřejmé, že se jedná o činnost, které se také ICT odborníci věnují většinu své pracovní doby.

Přechodem ke cloudovým službám se jim tedy mohou „uvolnit ruce" pro jiné činnosti, jež mohou přinést větší užitek a zkvalitnění služeb.

3.6.3. Zvýšení přístupnosti pomocí mobilních zařízení

Příležitost plně navazující na již zmíněnou silnou stránku cloudových služeb. V rámci tohoto oddílu alespoň zmíníme jeden dosud částečně opomíjený faktor a to je stále výraznější užívání přenosných zařízení („chytré" mobilní telefony, tablety, elektronické čtečky atd.) koncovými uživateli. Aplikace pro mobilní zařízení jsou na využití cloud computingu často přímo postavené. Mobilní zařízení zde vystupuje jako tenký klient, který pouze posílá požadavky na vzdálený server, jež provede požadované úkony a uživateli je zobrazen výsledek.

Jak říká analytik IDC Petrůj [2014]: „Mobilní aplikace jsou ideální u informací, k nimž je potřeba přistupovat každodenně: jízdní řády veřejné dopravy, možnosti parkování ve městech, předpověď počasí, turistické informace pro návštěvníky a podobně." Cloudové aplikace jsou pro tato řešení ideální. Jak bylo popsáno v PESTL analýze (VIZ KAP), dle DESI indexu je právě přístupnost a dostupnost informací a služeb veřejné správy v ČR na velmi nízké úrovni.

Počet uživatelů v ČR, kteří na Internet přistupují skrze mobilní zařízení, dosáhl v roce 2015 již 4 milionů [NETMONITOR, 2015].

3.6.4. Jednodušší spolupráce

Data jsou v cloudovém prostředí uloženy na jednom místě (tedy z pohledu koncového uživatele) a mohou být dostupná odkudkoliv a to pro všechny oprávněné uživatele zároveň. Data tak nejsou „roztříštěna" v různých informačních systémech nebo přímo na discích jednotlivých zaměstnanců, čímž je zamezeno provádění duplicitní práce.

Využití cloudových služeb také vede k zjednodušení spolupráce (např. v reálném čase editovat jeden společný dokument) a data a jsou uživatelům neustále dostupná v aktuální verzi.

3.7. Hrozby

3.7.1. Bezpečnostní rizika

Cloud Security Alliance v roce 2013 vydala seznam 9 největších hrozeb pro cloud computing [CSA, 2013]. Na následujících řádcích je představeno 6 hrozeb (nejvíce relevantních pro veřejný sektor) představeny v pořadí, v jakém se v reportu objevily, avšak popsány z hlediska jejich vlivu na využití cloud computingu v institucích veřejného sektoru.

- **Krádež dat**

Data uložená v cloudu jsou častým terčem útoků. Nejedná se pouze o osobní data, ale prakticky o jakákoliv data, která mohou mít pro útočníky nějakou hodnotu.

Zde je však třeba upozornit, že v druhém případě se jedná především o problém, s kterým se potýká soukromý sektor. Následky úniku podnikových dat mohou vést k velkým finančním ztrátám, případně i k ohrožení. Data a informace veřejného sektoru podléhají zákonu č. 106/1999 Sb., o svobodném přístupu k informacím (VIZ KAP) a jejich případný únik by neměl pro instituce veřejného sektoru představovat vážné (či snad žádné) riziko. Jiná situace nastává při úniku osobních údajů, které podléhají zvláštní ochraně.

- **Ztráta dat**

Ztráta dat, ačkoliv v žebříčku CSA na druhém místě, je pro veřejný sektor patrně větší hrozbou než jejich únik. To právě s ohledem na výše zmíněný zákon č. 106/1999, kdy při ztrátě dat by tak nemohlo dojít k naplnění povinností z tohoto zákona vycházejících. Ke ztrátě může samozřejmě dojít i při jejich úniku, kdy se například útočník rozhodne pro další poškození uživatele a data smaže.

Ztráta dat může mít i jiné příčiny než napadením z vnějšku. K pochybením vedoucích ke ztrátě dat může nastat na straně poskytovatele i uživatele služeb.

Uživatel si může přivodit ztrátu dat např. ve chvíli, kdy ukládá data do cloudu v šifrované podobě a ztratí klíč pro jejich rozšifrování. Na straně poskytovatele k takové ztrátě může dojít např. při fyzickém poškození infrastruktury způsobeném třeba přírodními živly.

Únik a ztráta dat nejsou problémy, které by hrozily pouze v cloudovém prostředí. Hrozby pro data se staly předmětem zkoumání studie americké společnosti Verizon [2014] specializující se na poskytování internetového připojení. Hlavní příčiny ztráty a úniku dat ve veřejném sektoru podle této studie jsou: „různé chyby" jako poslání dat nesprávným příjemcům; specializované kriminální softwarové aplikace („crimeware"); vlastní zaměstnanci; fyzická krádež dat, ať už v podobě zaměstnanců odnášejících si citlivé údaje na USB discích, či nechtěná ztráta pracovního počítače; kybernetická špionáž.

Naprosté zabezpečení a úplné vynulování rizik spojených s únikem a ztrátou dat patrně není a nebude možné. Přesto se tato rizika dají minimalizovat nebo alespoň zmírnit. Část odpovědnosti leží na poskytovateli, který by se měl starat především o technologická řešení bezpečnosti (anti-virový software, firewall apod.), kontinuální monitoring a také zajistit organizační prvky zabezpečení, tedy že k datům budou mít přístup pouze oprávnění

zaměstnanci poskytovatele. Odpovědnost poskytovatele za technologické zabezpečení pochopitelně stoupá i v závislosti na poskytovaném servisním modelu a tedy spravované části infrastruktury. Odpovědnost a sankce by měly být jasně stanoveny v rámci smluvního vztahu mezi poskytovatelem a uživatelem (viz legislativní okruh PESTL analýzy).

Uživatel musí předcházet rizikům se stejnou důsledností jako poskytovatel. Technologické i organizační prvky zabezpečení musí zajistit i na své straně.

- **Krádež uživatelských účtů**

Nejedná o hrozbu spojenou výlučně s cloudovými službami, ale právě v cloudovém prostředí, kdy jsou data a aplikace (virtuálně) na jednom místě a přístupné odkudkoliv, se mohou následky mnohonásobně zvýšit oproti klasickému IT prostředí.

Techniky pro krádež účtů jsou rozmanité, od hrubé síly (tzv. brute-force attack), kdy se útočník snaží odhalit heslo pomocí testování různých kombinací, přes využívání různých bezpečnostních děr webových technologií, až v poslední době po stále rozšířenější „phishing" (podvodné získání přístupových údajů pomocí elektronické komunikace) [CSA, 2013].

Pro předcházení rizik spojených s krádeží uživatelských účtů je třeba v rámci organizace nastavit politiku využívání silných hesel (nejméně 8 znaků, nesmí obsahovat uživatelovo jméno a nejlépe žádné celé slovo, využít malá i velká písmena, číslice a speciální znaky) s jejich pravidelným střídáním. V závislosti na míře kritičnosti poskytované služby je také vhodné zvážit a případně nasadit dvou faktorovou autentizaci (obvykle heslo a jeden další způsob, jako např. zaslání potvrzovacího kódu pomocí SMS, případně využití biometrických údajů).

- **Nezabezpečená API**

Pro komunikaci a správu cloudových služeb jsou využívána programovací rozhraní (API), která jsou potenciálně napadnutelná a mohou být příčinou výše zmíněných rizik, ale také celkového ohrožení cloudové služby jako takové [CSA, 2013].

Úroveň odpovědnosti za dostatečné zabezpečení se mění v závislosti na využitém servisním modelu. Čím vyšší úroveň, tím vyšší odpovědnost poskytovatele služeb a obráceně. Je však především na uživateli, aby si vybral poskytovatele, který dokáže garantovat patřičné zabezpečení.

- **Odmítnutí služby (Denial of Service, DoS)**

Odmítnutí služby je napadením jednoho (označováno zkratkou DoS), případně více útočníky (označováno zkratkou DDoS, Distributed Denial of Service, distribuované odmítnutí služby) s účelem zamezení přístupu uživatelů ke službě. Útočníci, jednoduše řečeno, zahrnou cílovou službu velkým počtem požadavků a snaží se vytvořit tak velký „provoz", který cílová služba není schopná odbavit. Pro konečné uživatele se tak služba jeví jako nedostupná nebo velmi pomalu reagující.

Vzhledem k poměrně jednoduchému provedení se jedná o častý způsob napadení služeb na Internetu a cloudové služby se stávají stále častějším terčem [LITHNICIUM, 2013]. Jedním z největších a nejznámějších DDoS útoků proběhl v roce 2007 na Estonsko, tedy na nejdůležitější estonskou infrastrukturu - služby veřejné správy, bankovnický sektor, ale i elektrárny [HERZOG, 2011].

Veřejné cloudové služby, ač jsou vyhledávaným terčem, mohou být vůči těmto útokům lépe vybavené a to díky své elasticitě a škálovatelnosti a platí to obzvlášť pro služby velkých poskytovatelů.

- **Vlastní zaměstnanci**

Dalším bezpečnostním rizikem, které je třeba alespoň stručně zmínit, jsou vlastní úmyslně škodící zaměstnanci (v angl. literatuře označování jako „malicious insiders"). Může se jednat o současného nebo bývalého zaměstnance, externího pracovníka apod., tedy o osobu s autorizovaným přístupem k informačním systémům organizace, který úmyslně zneužívá svého přistupu k osobnímu obohacení, případně poškození samotné organizace [CSA, 2013].

Ani v tomto případě se nejedná o riziko spjaté výhradně s cloud computingem. V rámci instituce je třeba nastavit takové prostředí, ve kterém mají zaměstnanci přístup pouze k částem služeb, které potřebují k výkonu své práce.

- **Zranitelnost sdílených technologií**

Služby veřejného cloudu jsou postavené na sdílení infrastruktury ve všech vrstvách (dle servisního modelu) mezi různými zákazníky poskytovatele. Pokud jednotlivé prvky, tvořící infrastrukturu, neposkytují dostatečně zabezpečené oddělení jednotlivých uživatelů (zákazníků), tak může být takovýto bezpečnostní nedostatek využit jedním z uživatelů k poškození ostatních, v extrémním případě rovnou k poškození celé cloudové infrastruktury.

V tomto případě odpovědnost za prevenci proti problémům způsobených zranitelností sdílených technologií leží především na poskytovateli cloudových služeb.

3.7.2. „Vendor lock-in"

Výhradní závislost na poskytovateli, označována nejčastěji anglickým termínem „vendor lock-in", je jednou z nejčastěji zmiňovaných hrozeb ve spojení s cloud computingem. Závislost nastává ve chvíli, kdy uživatel není schopen převést svá data a aplikace k jinému poskytovateli či zpět do své vlastní IT infrastruktury, případně toho není schopen bez velkých finančních nákladů. Vzhledem k povaze cloud computingu je výskyt závislosti na jediném poskytovateli vyšší než u klasického IT prostředí.

Pravděpodobnost uzamknutí se u jediného poskytovatele se zásadně zvyšuje, pokud jsou poskytované cloudové služby postaveny na proprietárních řešeních a nevyužívají otevřené standardy (VIZ KAP).

Dalším faktorem, který může vést k uzamknutí se u jediného poskytovatele je neexistující „exit strategie".

Riziko uzamknutí se u poskytovatele je společné pro všechny servisní modely cloud computingu.

Že se nejedná pouze o teoretickou hrozbu, ale o reálný problém, se kterým se potýká i veřejný sektor, dokládají současné problémy hl. města Prahy s technologií OpenCard. V tomto případě se jedná o kauzu exemplárně demonstrující, jak vypadá uzamknutí se u jediného poskytovatele, způsobené špatně nastavenými smlouvami a využitím proprietárních technologií[29], a k jakým potížím může vést. V tomto případě se sice nejedná o cloudovou službu, ale princip uzamknutí se u poskytovatele je totožný.

4.7.3. Nedostatečná připravenost

Podcenit přípravu na přechod ke cloudové službě je nejlepší cestou k totálnímu fiasku implementace. Je třeba předem patřičně zvážit všechna rizika, ohodnotit současný stav ICT v rámci organizace a zajistit návaznost na používané informační systémy, připravit plán migrace, plán exitu atd. Doporučený postup je popsán v životním cyklu cloudových služeb.

Mít vše připravené předem je nejlepší způsob, jak využít všech výhod cloud computingu.

3.7.4. Chybějící zkušenosti

Ve veřejném sektoru v ČR není cloud computing zatím příliš rozšířen, až na některá SaaS řešení v podobě např. kancelářských aplikací. Přesná statistická data sice nejsou v této

[29] Jedná se samozřejmě o zjednodušení situace.

oblasti známá (ČSÚ zatím sleduje pouze využití cloud computing v podnicích), ale alespoň v dostupné literatuře nelze prakticky nalézt žádné případové studie, ze kterých by mohly ostatní instituce čerpat zkušenosti.

3.7.5. Nepřehledná situace v ICT politice státu

V rámci PESTL analýzy byla rozebrána politika ČR v oblasti ICT. Ta je velice nestálá a nepřehledná, což může negativně ovlivňovat rozhodnutí, zda využít cloudové služby.

V současnosti se zdá, že se chystá stavba privátních datových center, která by poskytovala služby institucím veřejné sektoru (minimálně státní správě). Z veřejně dostupných zdrojů se však nedá s jistotou říct, o jaké služby se bude jednat a jaké instituce budou oprávněny jejich služby využívat.

3.7.6. Špatné smluvní podmínky

Vyjednání smluvních podmínek, které budou prospěšné a vyhovující pro obě strany je náročná činnost, která se neobejde bez právní pomoci a zároveň spolupráce s vlastním ICT oddělením. Velký důraz by měl být kladen na SLA, jejíž správné nastavení zajišťuje dodání služby v takovém rozsahu a podobě, v jaké je vyžadována.

Smluvním podmínkám byl věnován oddíl v rámci legislativního okruhu PESTL analýzy.

3.7.7. Kulturní bariéry v rámci organizace

S překonáním kulturních bariér v rámci organizace měly problém instituce veřejného sektoru v USA, jak zdokumentoval report GAO [2014]. Představitelé tamních institucí nejevili ochotu přecházet na nový způsob práce s informačními technologiemi a vyrovnávat se s novými riziky.

Veřejný sektor je obecně méně ochotný podstupovat rizika než privátní sféra. V případě kladného výsledku případného podstoupení rizika v privátní sféře je obvykle vyšší zisk a z toho plynoucí odměny pro odpovědné osoby. Opačný výsledek může mít pochopitelně negativní následky, ale většinou existuje nějaký rozumný poměr mezi rizikem a případným ziskem. To, jak upozorňuje studie poradenské společnosti KPMG [2012], ve veřejném sektoru úplně neplatí. V případě kladného výsledku se mohou odpovědní pracovníci dočkat pochvaly[30], ale příliš více očekávat nemohou. Na druhou stranu, v případě neúspěchu mohou být následky daleko horší. Není zde tedy úplně vyrovnaný poměr mezi hrozbou a odměnou.

[30] Případně nějaké finanční prémie, ale co se udělování prémií ve veřejném sektoru (především veřejné správě) týče, jedná se o nejistou a ne zcela průhlednou záležitost.

4. Implementace Office 365 na FF UK - případová studie

4.1. Úvod

V rámci této kapitoly je popsána implementace Office 365 společnosti Microsoft na Filosofické fakultě Univerzity Karlovy v Praze (dále FF UK) a to především s ohledem na jejich „cloudovou" funkcionalitu. Nejprve jsou stručně představeny subjekty, které se na implementaci podílely. Dále je popsán průběh výběrového řízení, které samotné implementaci předcházelo. Následující část se věnuje samotným implementovaným službám a poslední část se zaměřuje na konkrétní problémy spojené se samotnou implementací.

4.2. Představení zúčastněných subjektů

Základními subjekty vystupujícími v této případové studii jsou FF UK, jež vystupuje v roli uživatele, Servodata a.s., jež vystupuje v roli zprostředkovatele a Microsoft Corporation v roli poskytovatele služeb (popis základních rolí je vysvětlen v úvodní kapitole).

4.2.1. Filosofická fakulta Univerzity Karlovy v Praze

FF UK byla založena v roce 1348 a je tak jednou z nejstarších evropských fakult vůbec. V současnosti na FF UK studuje cca 8.000 studentů v téměř 70 oborech. Zaměstnanců fakulty je přibližně 750 [HÁJEK, 2014]. Jednotlivé katedry a ústavy FF UK jsou rozprostřeny v 10 budovách v Praze.

FF UK hospodaří s vyrovnaným rozpočtem. Poslední veřejně dostupné údaje pocházejí za rok 2013, kdy celkové náklady fakulty byly cca 665 mil. Kč a výnosy cca 670 mil. Kč.

Správu a rozvoj informačních technologií má na starosti Laboratoř výpočetní techniky FF UK. V roce 2013 spravovala 28 serverů, cca 700 fakultních počítačů, stovky pracovních notebooků přidělených zaměstnancům a další HW vybavení (např. tiskárny). Kromě HW má na starosti také SW vybavení, mezi které patří intranet fakulty, který je postaven na cloudové službě MS SharePoint Online, kancelářské aplikace v cloudu Office 365 a cloudové úložiště OneDrive. Tyto SW produkty, jejich implementace a využití jsou hlavním tématem této případové studie.

4.2.2. Servodata, a.s.

Akciová společnost Servodata byla založena již v roce 1991. Sama sebe charakterizuje jako společnost „specializující se zejména na řešení podnikové infrastruktury - nabízí komplexní

HW i SW řešení a služby pro ukládání, správu a zajištění bezpečnosti dat, stejně jako kompletní licenční správu“ [SERVODATA, 2013]. Svými obchodními aktivitami společnost cílí především na veřejný sektor. Portfolio zahrnuje především správu licencí a řešení od Microsoftu.

Společnost je držitelem několika ISO certifikací, zejména Systému řízení bezpečnosti informací 27001:2005 a Systému řízení jakosti ISO 9001:2000.

Z hlediska této studie je také podstatný obchodní vztah mezi Servodata, a.s. a Microsoftem. Servodata, a.s. je držitelem statusu „Licensing Solution Partners”, který je udělován na základě specifických regionálních požadavků a označuje doporučené partnery pro poskytování produktů Microsoft prostřednictvím licenčních programů [MICROSOFT, 2015a].

Servodata, a.s. je výherce výběrového řízení (viz následující podkapitola) o dodání „softwarových licencí a souvisejících služeb pro osobní počítače a servery”.

4.2.3. Microsoft Corporation

Microsoft Corporation (dále jen Microsoft), založená v roce 1975, je jednou z největších a nejznámějších společností působících na poli informačních technologií. Nejznámějšími produkty jsou operační systém Windows, kancelářské aplikace Office či herní konzole Xbox. Na trh s cloud computingem vstoupil Microsoft v roce 2010, kdy zpřístupnil pro širší využití svoji službu Windows Azure (dnes Microsoft Azure) poskytující servisní modely IaaS a PaaS [HAUGER, 2010].

Microsoft je držitelem řady certifikátů, z nichž jsou pro tuto studii relativní certifikáty získané pro produkt Office 365:

- ISO 27001
- Safe Harbor
- FISMA
- ISO 27018

4.3. Příprava a realizace implementace

V úvodní kapitole byl popsán životní cyklus cloudových technologií, který v rámci této podkapitoly využijeme pro popis implementace cloudových služeb na FF UK.

4.3.1. Iniciační fáze

První zmínky o využití cloudových služeb lze nalézt v dokumentu Aktualizace Dlouhodobého záměru FF UK pro akademický rok 2012/2013, ve kterém je stanoven úkol: *„Připravit a realizovat projekt převedení vybraných IT služeb a aplikací na cloud computing*." Od jehož splnění se očekávalo: *„zlepšení komfortu a úrovně zajištění služeb správy dat a možnosti IT na fakultě, a to bez investic do nových serverů*" [STEHLÍK, 2012].

První přípravné kroky pro zavedení cloud computingu byly učiněny již v říjnu 2012. Do datových center měly být přesunuty poštovní služby, intranet a další aplikace. Kromě očekávání lepší dostupnosti a větší spolehlivosti služeb k této změně došlo také v souvislosti s novou licenční politikou - tzv. multilicencemi umožňujícími získávat kancelářský software v posledních verzích, průběžně upgradovat a zaměstnancům na plný úvazek používat tento SW i na soukromých počítačích [FF UK, 2012].

Iniciační fáze skončila vytvořením zadávací dokumentace a zahájením zadávacího řízení.

4.3.2. Akvizice

Zadávací řízení pro veřejnou zakázku na dodávky s názvem „Softwarové licence a související služby pro osobní počítače a servery" bylo zahájeno 15. 7. 2013. Druhem zadávacího řízení bylo zvoleno zjednodušené podlimitní řízení[31], protože maximální možnou nabídkovou částkou zakázky byla stanovena hodnota 2.000.000,00 Kč.

Zadávací dokumentace, kromě maximální hodnoty zakázky a dalších formálních požadavků, stanovuje technické podmínky poptávaných služeb a kvalifikační předpoklady dodavatele, ze kterých budou představeny ty nejdůležitější.

Technické kvalifikační požadavky stanovily pro dodavatele nutnost mít k dispozici alespoň 2 osoby splňující následující odborné kvalifikace:

- *„Designing and Providing Volume Licensing Solutions to Large Organizations".*
- *„Designing, Assessing, and Optimizing Software Asset Management".*
- *„Certified Trainer".*

Hlavním předmětem zakázky byly licence na softwarové produkty (z tohoto důvodu se jednalo o veřejnou zakázku na dodávky a ne o veřejnou zakázku na služby), jež měly vyhovovat těmto požadavkům:

[31] Ve zjednodušeném podlimitním řízení vyzývá veřejný zadavatel písemnou výzvou nejméně 5 zájemců k podání nabídky a k prokázání splnění kvalifikace. Zadavatel je však povinen přijmout a hodnotit i nabídku dodavatele, který nebyl vyzván.

- SW licence a související služby pro 720 zaměstnanců.
- SW musí být kompatibilní se stávajícím ICT prostředím zadavatele (=servery i koncové stanice na platformě produktů Microsoft).
- Komponenty SW - kancelářský SW (textový editor, tabulkový procesor, aplikace pro tvorbu prezentací, databázová aplikace, aplikace pro tvorbu marketingových materiálů, poštovní klient).
- Licence pro základní serverový operační systém, potřebný SW pro správce sítě, server elektronické pošty.
- Hlavní předmět zakázky byl dále doplněn o požadavek na tyto služby:
- SW služba zajišťující zadavateli možnost zřídit studentům a zaměstnancům emailové a souborové schránky a komunikaci. Emailové schránky o kapacitě alespoň 25 GB pro uživatele (s možností navýšení) a úložiště s možností spolupráce o velikosti alespoň 500 MB na uživatele s přístupem přes Internet. Dále služba měla umět zasílání rychlých zpráv, hlasovou komunikaci, video chaty, prohlížení souborů přes webové stránky a jejich úpravu. V rámci této služby byla také požadována možnost zřízení minimálně 4.000 uživatelských účtů.
- Dále byl stanoven požadavek na technickou podporu produktů, školení uživatelů a další konzultační služby.

První 4 body předmětu zakázky požadují licence na víceméně standardní kancelářský software, jehož technické parametry by mohly splnit např. i některé „open source" aplikace. Z pohledu této práce je mnohem zajímavější první bod požadovaných služeb. Zde se již jedná o požadavky, které mohou splnit prakticky pouze cloudové služby vzhledem k jejich definujícím charakteristikám.

Výše zmíněné technické kvalifikační předpoklady dodavatele, ač to samotná specifikace neuvádí, představují certifikace vydávané společností Microsoft obchodníkům, kteří prodávají licence a zprostředkovávají služby společnosti Microsoft. Tím prakticky došlo k limitaci poptávaných licencí a služeb na produkty této společnosti.

Výhercem veřejné zakázky se stala, již představená, firma Servodata, a.s., se kterou byla uzavřena rámcová smlouva dne 26. 8. 2013 na 3 roky. Nabídková cena za požadované dodávky a služby činila 1.748.037,00 Kč. Skutečná cena zaplacená za 3 roky bude patrně

vyšší, ale v současné době není známá (alespoň ne z veřejných zdrojů) a zadavatel nemá povinnost skutečnou cenu zveřejnit, pokud nepřesáhne 5 mil. Kč, jak stanoví ZVZ.

Servodata, a.s. dodala FF UK softwarové produkty společnosti Microsoft, jež přesně odpovídají požadavkům zadávací dokumentace. Z pohledu této studie jsou podstatné následující produkty a služby:

- **Office Professional Plus**

Kancelářský balík obsahující Microsoft Word (textový editor), Excel (tabulkový editor), PowerPoint (SW pro tvorbu prezentací), Outlook (emailový klient), OneNote (poznámkový editor), Publisher (textový a především grafický editor), Access (nástroj pro správu relačních databází), InfoPath (SW pro vytváření formulářů). Tyto aplikace jsou provozovány na pracovních stanicích uživatelů.

- **Office 365 (plán A2)**

Cloudová služba Office 365 je pro akademické instituce dostupná v několika verzích (tzv. plánech). V tomto případě byla dodána ve verzi A2 (dnes odpovídá verzi E2), jež je pro akademická instituce dostupná zdarma. Plán A2 obsahuje Office Online, Sharepoint Online, Exchange Online, OneDrive a Lync Online.

- Office online
- Office online obsahuje webové verze těchto kancelářských aplikací:
- Word
- Excel
- Powerpoint
- OneNote
- Outlook
- Kalendář

Všechny tyto aplikace jsou umístěny na serverech Microsoftu. Ve webové verzi chybí Office aplikace Publisher, Access a InfoPath.

- **OneDrive**

Služba zpřístupňující webové úložiště uživatelům, do kterého je možné nahrávat dokumenty Microsoft Office a pracovat na nich v online módu pomocí aplikace Office online.

- **SharePoint Online**

Webová aplikace sloužící k vytváření intranetu, sdílení a vytváření dokumentů mezi uživateli napříč organizací. Stejně jako online aplikace Office 365 je SharePoint provozován na serverech Microsoftu.

- **Exchange Online**

E-mailový server hostovaný na serverech Microsoftu. Uživatelé mají v základní verzi dostupné účty s úložným prostorem 25 GB. Server je obvykle propojen s aplikací Outlook (ve webové i desktopové verzi), ale pro přístup je možné použít i jiné klienty (např. Thunderbird). Server je chráněn anti-virovým a anti-spamovým softwarem.

- **Lync Online**

Aplikace pro telefonování, videohovory, posílání instantních zpráv, tvorbu online konferencí pro zaměstnance i lidi z vnějšku.

Všechny výše zmíněné služby jsou poskytnuty v multilicenčním programu EES (Enrollment for education solutions) pro větší akademické instituce [MICROSOFT, © 2015]. Součástí této licence je tzv. „Software Assurance", která zajišťuje právo na nejnovější verze softwaru, což je důležité především pro desktopové aplikace (online aplikace v cloudu jsou aktualizovány průběžně a automaticky).

4.3.3. Implementace

Vzhledem k spíše ilustračnímu charakteru této případové studie nebudou popisovány technické detaily implementace, avšak stručně se zaměříme alespoň na jeden prvek implementace a to správu identit a přístupových hesel.

Dále je také třeba zmínit, že implementace je stále probíhající proces. V současnosti mají zaměstnanci dostupný intranet (na platformě Sharepoint), úložiště OneDrive, webové i desktopové aplikace Office a emailové schránky v cloudu.

Některé funkce však ještě nejsou uživatelům dostupné, a není tak využito veškerých služeb, na které má fakulta dle licence nárok. Uživateli, kteří mají dle licence nárok na služby, nejsou pouze dosud zmiňovaní zaměstnanci, ale také studenti fakulty. Ti však dosud služeb Office 365 využívat nemohou z důvodů, které jsou vysvětleny na konci této podkapitoly.

- **Správá identit a přístupů**

Nyní k samotné implementaci. Služby jsou provozovány v cloudu (tedy na serverech Microsoftu), a tak odpadá komplikované nastavování serverového prostředí na straně instituce. Některé záležitosti však zůstávají čistě v rukou (resp. serverech) fakulty. V tomto případě je jednou z nich správa identit a přístupů.

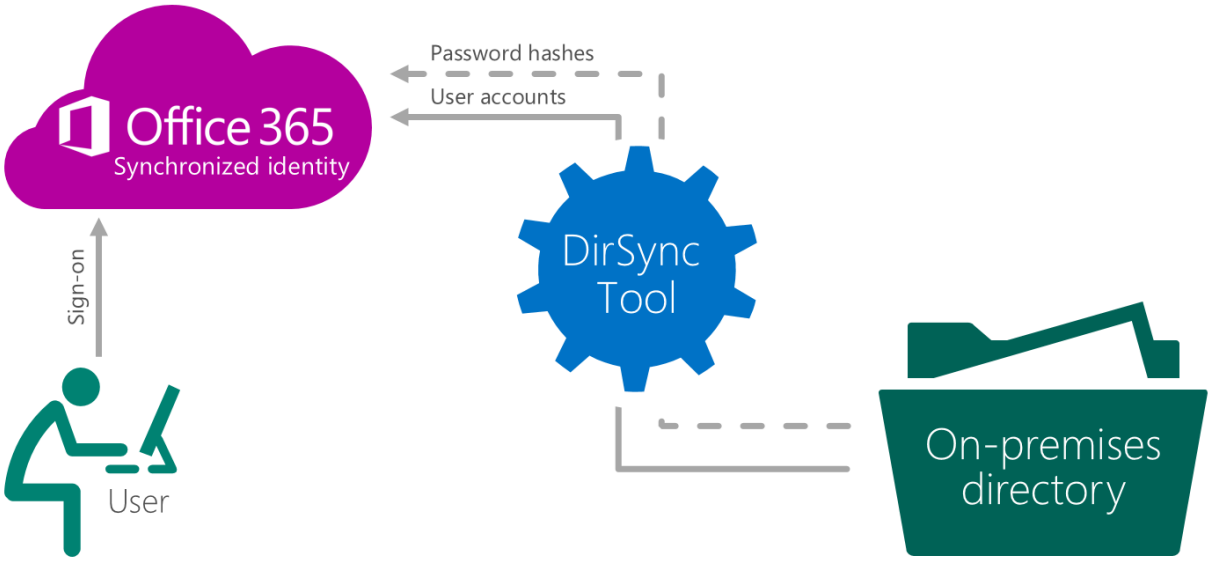
Microsoft svým zákazníkům poskytuje výběr ze 3 modely řešení správy přístupových údajů pro své cloudové služby:

- Identita v cloudu
- Synchronizovaná identita
- Federovaná identita

První model je pro organizace, které nemají žádný centrální adresář přístupových údajů a ty jsou tak spravovány a uloženy v cloudu.

Druhý model je pro organizace, které mají vytvořený centrální adresář přístupových hesel. Právě tento model je momentálně využíván na FF UK. Přihlašovací údaje jsou spravovány v Centrální autentizační službě UK (CAS). Uživatel se ke službám Office 365 přihlašuje svými údaji z CAS, které jsou synchronizovány do nástroje „Microsoft Azure Active Directory Sync Tool" (zkráceně DirSync), vůči kterému si Office 365 ověří správnost zadaných údajů (viz obrázek níže). Samotná autentizace a autorizace uživatele tak v rámci tohoto modelu probíhá v cloudu. Tento model nasazení správy identit umožňuje rozlišení jednotlivých uživatelských skupin, které tak mohou mít různá přístupová a administrátorská oprávnění (např. v rámci intranetu). Nevýhodou tohoto modelu je, že nepodporuje zavedení „single sing-on" (SSO) prostředí napříč různými aplikacemi provozovaných v rámci instituce[32] [ANDREW, 2014].

[32] Služby Office 365 je však po přihlášení možné využívat všechny, ale např. pro přihlášení k Portálu elektronických zdrojů je nutné zadat přihlašovací údaje znovu.



Zavedení prostředí SSO je naopak možné v rámci třetího modelu - Federace identit. V rámci tohoto modelu se uživatel přihlašuje také svými údaji, jež jsou spravovány v adresáři své domovské instituce, ale samotná autentizace a autorizace neprobíhá v cloudu, ale je prováděna poskytovatelem identity, což může být „on-site" server nebo třetí strana[33] (viz obrázek č. 3). Z hlediska funkčnosti a uživatelského pohodlí je tento model nejvýhodnější, ale zároveň vyžaduje zajištění vysoké dostupnosti serverů, na kterých probíhá autentizace uživatelů. O nasazení tohoto modelu se na FF UK uvažuje, ale právě hrozba výpadků „on-site" serverů je jedním z důvodů, proč se tak ještě nestalo [Tichý, 2015].

- **Intranet a osobní úložiště OneDrive**

Intranet, tedy interní web přístupný pouze zaměstnancům fakulty (případně i externistům s patřičným oprávněním), je postaven na službě SharePoint. Struktura intranetu je koncipována tak, aby odpovídala „externímu" webu a zaměstnanci se v jeho rámci mohli intuitivně orientovat.

Každá funkční složka fakulty[34] (a její patřičné podsložky) má vytvořenou svoji vlastní stránku, na kterých mohou být publikovány dokumenty dané složky pro všechny zaměstnance a zároveň interní dokumenty dostupné pouze zaměstnancům dané složky [FF UK, 2014a].

[33] Na stejném principu funguje přihlašování ke vzdáleným zdrojům pomocí technologie Shibboleth, jež je na UK implementován.

[34] Funkčními složkami se rozumí jednotlivá oddělení a jejich podsekce (konkrétně katedry a ústavy, děkanát, knihovna, oborové knihovny, kolegium děkana, komise, centra a specializovaná pracoviště)

Z intranetu je možné lehce přejít do osobního úložiště OneDrive, které nyní poskytuje každému uživateli kapacitu 1 TB. Toto úložiště je možné synchronizovat s různými koncovými zařízeními uživatele a mít tak uložené soubory dostupné prakticky odkudkoliv. Soubory lze jednoduše vytvářet rovnou v prostoru OneDrive pomocí webových aplikací Office 365 [FF UK, 2014b].

- **Implementace služeb pro studenty**

V rámci licence by studenti měli mít přístup ke všem službám (kromě možnosti instalace desktopových aplikací Office Professional). Tatím tomu tak ovšem není. Důvody prozatímní nedostupnosti služeb pro studenty vysvětluje proděkan pro informační zdroje Tichý [2015]: „ *Zádrhel je v poněkud absurdní oblasti – abychom mohli studentům zpřístupnit licence Office365 případně jim zpřístupnit úložiště OneDrive, museli bychom je jako uživatele importovat do SharepointOnline. To by znamenalo, že při práci se Sharepointem (intranetem) budou figurovat ve všech seznamech osob, např. při výběru uživatelů sdílení atp. To by znamenalo zásadní problém při práci zaměstnanců – již nyní je při výběrech někdy problém, kdy existují zaměstnanci se stejným jménem i příjmením. To by se po importu dalších 10 tis. uživatelů znásobilo. Tzv. People Picker* (nástroj pro výběr uživatelů nebo skupin uživatelů - pozn. autora) *neumožňuje zobrazit další parametry uživatelů (např. akademické tituly, funkce apod.), které by výběr stejně se jmenujících osob usnadnily. Neumožňuje ani část uživatelů skrýt.* „ Jak proděkan dodává, tento nedostatek je potvrzen i Microsoftem, který zatím nedodal žádné řešení.

V brzké době se alespoň počítá se zpřístupněním ostatních služeb pro studenty, kteří ale nebudou integrováni do SharePointu.

5.3.4. Provoz

Jako první byl spuštěn provoz intranetu na začátku roku 2014, k čemuž se postupně přidávají další služby, jako emailový účet v cloudu. Přesná statistická data využívanosti jednotlivých služeb nejsou autorovi práce známé, ale přesto můžeme alespoň zhodnotit, jaké možnosti svým uživatelům přináší:

- K používání jsou vždy dostupné nejaktuálnější verze služeb.
- Velká úložná kapacita (momentálně 1 TB)
- Možnost vytváření, sdílení dokumentů a spolupráce na jejich tvorbě mezi zaměstnanci fakulty

- Aplikace Office 365 jsou dostupné pro různá koncová zařízení, prakticky bez omezení OS.
- Non-stop přístup ke službám a skrze webové rozhraní.

Ukončení

Provoz cloudových služeb na FF UK do své poslední fáze, tedy ukončení, ještě nedošel. Současná smlouva je platná do poloviny roku 2016, ale dá se předpokládat, že bude obnovena (za nových podmínek daných opětovným provedením výběrového řízení pro veřejnou zakázku) a ve využívání služeb se bude nadále pokračovat.

5.3.5. Shrnutí

Služby Office 365 bezpochyby již nyní přináší pro fakultu a její zaměstnance mnoho užitečných funkcí a možnosti se patrně budou dále rozšiřovat. Zatím však není využit plný potenciál, který tato služba nabízí. Patrně největší slabinou dosavadního stavu je nedostupnost služeb pro studenty, i když dle licence na to mají nárok.

Prozatím nevyužitý potenciál má také např. služba SharePoint, která se dá využít pro daleko širší spektrum služeb než je pouhý intranet. V rámci SharePointu lze např. automatizovat mnohé interní pracovní procesy, jak popisuje např. Urban [2012]. Příležitostí pro rozvoj služeb je tak nepochybně stále mnoho a do budoucna budou dále prozkoumávány.

Výše zmíněné skutečnosti autor rozhodně nezamýšlí jako kritiku současného stavu. Je pochopitelné, že implementace takto komplexního prostředí, jaké služba Office 365 nabízí, není jednoduchou a rychlou záležitostí. Z toho plyne i ponaučení, že rychlost nasazení, tedy jedna z často udávaných výhod cloud computingu (viz SWOT analýza) je značně relativní a velmi záleží na komplexnosti dané služby i organizačního prostředí instituce, pro kterou je služba zaváděna. Pozitivní však je, že jednotlivé funkční bloky lze uvádět do provozu postupně.

Nabízí se také otázka, zda fakultě nehrozí „vendor lock-in" u Microsoftu. Do jisté míry hrozí, ale to není problém pouze FF UK, ale prakticky hrozba pro celý veřejný sektor, jež primárně využívá kancelářské aplikace Microsoft. Avšak je třeba zmínit, že služby Microsoft jsou stále více interoperabilní a jejich použití se už zdaleka neomezuje pouze na zařízení s operačním systémem Windows. Využití zde zmíněných cloudových služeb je možné skrze všechny nejrozšířenější webové prohlížeče (Internet Explorer, Mozilla Fireforex, Google Chrome či Opera) bez omezení operačního systému, na kterém jsou provozovány.

V rámci této diplomové práce by také velký prostor věnován legislativním povinnostem spojených s ochranou osobních údajů v cloudovém prostředí. Z tohoto pohledu žádný rozpor s právem nehrozí, protože Microsoft poskytuje prakticky všechny myslitelné záruky. Podobná situace je i v oblasti bezpečnosti. Obě skutečnosti jsou doloženy seznamem certifikací Microsfotu,

Na závěr zbyla oblast, jež je v souvislosti s cloud computingem skloňována snad nejčastěji, jíž jsou finanční úspory. Zde však autor přiznává, že nemá k dispozici dostatek údajů pro vyslovení závěru, zda je současný model finančně výhodnější. V rámci ceny za licence na provoz Office 365 je i řada služeb, které nebyly dříve k dispozici (např. takřka neomezený úložný prostor pro data), a výhod jako lepší možnosti spolupráce na tvorbě dokumentů. S provozem dále nejsou spojeny nepřímé náklady, které by bylo nutné jinak vynaložit (cena serverů, náklady na provoz a údržbu, energetická náročnost atd).

Závěr

Cloud computing je již poměrně jistě etablovanou technologií, či přesněji řečeno způsobem poskytování ICT zdrojů v podobě služby. O tom svědčí např. fakt, že odborná diskuze se již přestala točit okolo snahy definovat samotný termín cloud computingu, ale přešla ke zkoumání praktických dopadů jeho využití. Široce uznávanou je definice NIST, která byla s minimálními úpravami přejata i Mezinárodní standardizační organizací.

Nyní k samotným závěrům vypracovaných analýz. Politický okruh PESTL analýzy představil politiku EU v oblasti cloudových služeb, „cloud-first" strategie USA a Velké Británie, dále byl stručně popsán přístup několika dalších evropských států a především politická situace v oblasti využití ICT ve veřejném sektoru.

Situace v České republice je značně nepřehledná a neustále se měnící. Druhou skutečnost autor práce shledává jako hlavní problém a to nejen ve vztahu k využití cloud computingu v institucích veřejného sektoru. Samotný cloud computing, v rámci strategických dokumentů obvykle označován jako sdílené služby, je zmiňován spíše okrajově, ačkoliv na jeho principu je, respektive by měla být, postavena architektura českého e-governmentu. Nejedná se však o využití služeb veřejného cloudu, který je hlavním tématem této práce. V plánu je postavení privátních řešení pro potřeby státní správy (a možná i pro širší využití). Vzhledem k tomu, jaké problémy zatím provázely většinu velkých ICT projektů státní správy, se autor obává, že ani tato realizace neproběhne bez problémů. Privátní cloud je sám o sobě velmi zajímavé řešení, které eliminuje některé problémy spojené s veřejným cloudem (ty jsou stručně zmíněné v úvodní části). Autor však nepředpokládá, že by státní správa byla schopná takové řešení vybudovat vlastními silami, ale stejně bude muset přizvat k pomoci i soukromé subjekty, které mají s budováním cloudových center zkušenost. Je tedy otázka, zda by nebylo výhodnější využít již existující infrastruktury veřejných cloudových služeb, např. pro zavedení virtuálního privátního cloudu (viz úvodní kapitola). V jednání je také možnost vytvoření tržiště se službami veřejného cloudu na jednom místě, tak jak je zavedeno ve Velké Británii pro tamní veřejný sektor. Tento způsob, jak ukázala analýza, je značně úspěšný.

Vývoj v ČR bude také do značné míry ovlivněn strategií UPCCE, kterou zavedla EU. V rámci politiky EU se cloud computingu dostává značné podpory, jako jednoho z hlavních bodů širší strategie Digitálni agendy pro Evropu.

Chybějící státní podpora využívání služeb veřejného cloudu nemusí být nutně překážkou pro jeho využívání. Jak ukázal rozbor situace v USA, tak ani povinnost přechodu ke cloudovým

službám nemusí být úplnou zárukou toho, že se tak stane. Hlavními překážkami v tomto případě byla vlastní kultura veřejných institucí, které neochotně zaváděly nové pořádky a zároveň velmi přísně nastavená bezpečnostní strategie. Jedno z nejdůležitějších ponaučení pro autora bylo, že pouhá pětina provedených implementací cloudových služeb přinesla finanční úspory. Hlavní motivací institucí veřejného sektoru pro akvizici cloudových řešení bylo zkvalitnění svých služeb a pracovních postupů.

Ekonomický okruh PESTL analýzy se věnoval výdajům na ICT v ČR, možnostem financování cloudových služeb, popsal nově se zavádějící systém v EU pro veřejné zakázky v předobchodní fázi a základní ekonomické termíny, které byly následně používány v rámci SWOT analýzy.

Dle provedené analýzy je financování ICT ve veřejném sektoru neprůhledné a ani v nedávné době zveřejněná data Ministerstva financí příliš nepomohla. Ve srovnání s okolními státy se však dá odvodit, že finance jsou vynakládány poměrně neúčelně. Dle agentury Deloitte jde dokonce cca 80 % výdajů do pouhé údržby a správy infrastruktury. Tyto výdaje představují oblast, ve které je využitím veřejného cloudu možné náklady snížit, protože tyto náklady jdou na vrub poskytovali služeb.

Možnosti financování cloudových služeb skrze fondy EU nejsou pro instituce veřejného sektoru příliš dosažitelné, protože tyto fondy jsou určeny pro podporu investičních nákladů. Výdaje za cloudové služby spadají do kategorie provozních nákladů.

Jako nejvhodnější model zpoplatnění cloudových služeb se jeví předplatitelský model, vzhledem k jeho nejjednodušší aplikaci ve výběrovém řízení.

Sociální okruh PESTL analýzy se zaměřil na odborné zázemí v podobě kvalifikovaných ICT pracovníků ve veřejném sektoru. Jak vyšlo najevo, odborníků je nedostatek na celém pracovním trhu. A vzhledem k tomu, že ICT odborníci ve veřejném sektoru mají nižší finanční hodnocení než jejich kolegové ze soukromé sféry, tak se příliv nových kvalifikovaných sil do veřejného sektoru nedá očekávat.

Zde autor opět vidí možný pozitivní přínos cloud computingu. Na straně poskytovatele stačí menší počet pracovníků, kteří se starají o ICT zázemí, jež může z definice cloud computingu využívat prakticky neomezený počet uživatelů. Zároveň přechod ke cloudu uvolňuje ruce ICT odborníkům zaměstnaných ve veřejném sektoru a ti se mohou věnovat přínosnějším činnostem než pouhé správě ICT infrastruktury instituce.

Technologický okruh analyzoval situaci v oblasti připojení k Internetu v ČR, jež je ze své podstaty naprosto zásadní podmínkou pro využívání cloudových služeb. Ta je ve stavu dobrém a žádná významná rizika pro využití cloud computingu nebyla identifikována. Druhou a podrobně zkoumanou oblastí byla standardizace cloudových služeb a certifikační schémata. Zde autor vidí jednu z velkých slabin současného stavu a to je především nejednoznačná shoda na otevřených standardech, což v důsledku zvyšuje riziko uzamknutí se u jediného poskytovatele. Naopak situace s certifikačními schématy potvrzujícími např. míru zabezpečení dat u poskytovatele je již velmi dobře ustálená.

Poslední okruh PESTL analýzy byl věnován právní problematice dotýkající se využívání cloudových služeb ve veřejném sektoru. Za hlavní problém bývá obvykle označována otázka předávání osobních a citlivých dat do cizích států, což je situace nastávající v cloudovém prostředí velice často. Existují právní instrumenty, které tento problém, alespoň z legálního hlediska, dokáží ošetřit. Mezi ně patří institut Safe Harbor pro data předávaná americkým společnostem a závazná korporátní pravidla pro velké mezinárodní společnosti. Velké a zavedené společnosti, které chtějí podnikat s cloudovými službami v Evropě, to mívají patřičně ošetřené a tento aspekt by neměl způsobovat větší překážky. Jiná situace je u cloudových služeb poskytovaných zdarma (např. různé sociální sítě), kdy je nutné věnovat patřičnou pozornost tomu, jaká data jim poskytnout.

Dobře nastavený smluvní vztah mezi uživatelem a poskytovatelem je naprostým základem pro využívání cloudových služeb. Rámcová doporučení byla popsána v rámci analýzy.

Povinností pro instituce veřejného sektoru je poptávání (nejen) cloudových služeb dle zákona č. 137/2006 Sb., o veřejných zakázkách. V tom autor vidí jedno z největších rizik či spíše bariér pro instituce veřejného sektoru. Tento zákon do jisté míry limituje možnost využití škálovatelného charakteru cloudových služeb, protože součástí zadávací dokumentace výběrového řízení musí být předpokládaná hodnota zakázky. To do značné míry limituje poptávání služeb modelu IaaS, pro nějž je značně problematické vypočítat předpokládanou hodnotu zakázky. Poněkud jednodušší situace je u produktů SaaS, jenž obvykle využívá modelu předplatného, jehož předpokládaná hodnota se dá poměrně jednoduše vyčíslit.

Ve třetí kapitole byla zpracována SWOT analýza vycházející z vlastností cloud computingu popsaných v úvodní části a zároveň navazuje na PESTL analýzu, která byla zdrojem pro část popisující příležitosti a hrozby spojené s využitím cloudových služeb.

Silné stránky spočívají především v energetické a ekonomické úspornosti plynoucí ze sdílení zdrojů mezi více uživateli. Další silnou stránkou je flexibilita, která umožňuje rychlé

přidávání a odebírání zdrojů dle aktuální potřeby a tím umožnuje i rychlé nasazení nových služeb.

Hlavní silné stránky z autorova pohledu představuje přesun většiny odpovědnosti za správu infrastruktury na stranu poskytovatele. To dává institucím veřejného sektoru možnost využití zkušeností, které tito poskytovatelé mají např. v oblasti zabezpečení svých služeb, nebo zálohování dat. Služby v cloudu mají také obvykle větší dostupnost než „on-site" ICT řešení, tedy nedochází tak často k výpadkům služeb.

Slabé stránky vycházejí částečně z PESTL analýzy a jsou jimi již zmíněné malé možnosti financování skrze EU fondy, neshoda na využití otevřených standardů mezi poskytovateli a závislost na připojení k Internetu.

Přínosy, které využití služeb veřejného cloudu může institucím veřejného sektoru přinést, se dají rozdělit do několika oblastí. První je oblast financí. Cloudové služby mohou přinést finanční úspory a to především snížením celkových nákladů vlastnictví, kdy služby převedené do cloudu již negenerují nepřímé náklady spojené s jejich provozem. Ne vždy, jak již bylo řečeno, jsou finanční úspory hlavním důvodem pro využití cloudových služeb. Hlavní přínosy ve finanční oblasti leží jinde a to především v zjednodušení jejich predikovatelnosti a snížení potřebných kapitálových investic potřebných při akvizici nového vybavení nebo služby. Ty představují velkou finanční zátěž a instituci mohou na nějakou dobu připravit o finanční prostředky na jiné a možná i potřebnější výdaje. ICT není obvykle hlavní činností, které se instituce veřejného sektoru věnují, ale přesto je jí věnována velká část rozpočtů a zároveň času. Obojí lze nepochybně využít lépe.

Nasazení cloudových služeb může také pomoci větší a jednodušší spolupráci mezi pracovníky organizace. Jako příklad může posloužit zprovoznění intranetu na cloudové platformě MS SharePoint Online, jež je popsána v závěrečné kapitole.

Rizika využití cloudových služeb vycházejí, kromě již výše zmíněných rizik vyplývajících z PESTL analýzy, především ze ztráty kontroly nad vlastními daty, která jsou vždy přesunuta na stranu poskytovatele služeb. V tomto případě se jedná o technologická bezpečnostní rizika, která hrozí i datům, jež má ve své správě uživatel/instituce. Pokud bude vybrán kvalitní poskytovatel, je dost pravděpodobné, že jeho systém zabezpečení předčí možnosti většiny institucí veřejného sektoru.

Další rizika pocházejí především z vlastního prostředí instituce. A to především podceněné plánování, špatné vyjednaní smluvních podmínek, neexistující exit strategie, která může vést k uzamknutí se u poskytovatele atd.

Konečné hodnocení dle autora, zda jsou služby cloud computingu vhodné pro využití institucemi veřejného sektoru, nemůže být úplně jednoznačné. Vždy je třeba zvážit konkrétní situaci dané instituce a její potřeby. Nedá se očekávat a ani doporučit, aby instituce převáděly do cloudového prostředí veškeré své ICT zdroje. Ideální je začít pomalými a bezpečnými kroky, jako je např. využívání podpůrných aplikací modelu SaaS, jež neohrozily kriticky samotnou činnost instituce. Model IaaS se jeví vhodný za současného stavu, např. pro zálohování dat. Nicméně

Na základě výše představených rizik a možných přínosů autor předpokládá, že cloud computing bude institucemi veřejného sektoru využíván stále více.

Odborných prací věnujících se využití cloudových služeb ve veřejném sektoru je stále malé množství, což ve větší míře platí pro veřejný sektor ČR. Z tohoto pohledu je práce stále aktuální (i tři roky po svém zadání). Jiná situace je v soukromém sektoru, který není tolik svázán právními regulacemi a ke cloudovým službám přistupuje již poměrně dlouho.

Bibliografické reference

ACCENTURE, 2013. *A new era for European public services: Cloud computing changes the game*. [online]. [cit. 2014-06-14]. Dostupné z: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-New-Era-European-Public-Services-Cloud-Computing-Changes-Game.pdf
AKAMAI, 2014. *State of the Internet: Q4 2014* [online]. [cit. 2015-04-08]. Dostupné z: http://www.akamai.com/dl/content/q4-2014-soti-a4.pdf

AL-ROOMI, May, Shaikha AL-EBRAHIM, Sabika BUQRAIS a Imtiaz AHMAD, 2013. Cloud Computing Pricing Models: A Survey. *International Journal of Grid and Distributed Computing* [online]. Vol. 6, no. 5 [cit. 2015-04-14]. DOI: http://dx.doi.org/10.14257/ijgdc.2013.6.5.09. Dostupné z:http://www.sersc.org/journals/IJGDC/vol6_no5/9.pdf

AMBRUST, Michael, et al. 2009. Above the Clouds: A Berkeley View of Cloud Computing. [online]. 2009, s. 1-23 [cit. 2014-06-14]. Dostupné z: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

ANON., 1972. *Auerbach Guide to Time Sharing*. Philadelphia: Auerbach. Dostupné z: http://bitsavers.trailing-edge.com/pdf/auerbach/GuideToTimesharing_Jan73.pdf

ANDREW, Paul, 2014. Choosing a sign-in model for Office 365. In: *Office Blogs* [online]. Microsoft, © 2015 [cit. 2015-04-14]. Dostupné z: http://blogs.office.com/2014/05/13/choosing-a-sign-in-model-for-office-365/

APOGEO, 2011. Stát vynakládá miliardy korun na IT neúčelně. *Auditorské, účetní a mzdové služby, daňové poradenství, znalecký ústav: APOGEO* [online]. Praha, © 2006 – 2015, 13.4.2011 [cit. 2015-04-08]. Dostupné z: http://www.apogeo.cz/apogeo-tiskove-zpravy/stat-vynaklada-miliardy-korun-na-it-neucelne-808/

ARIF, Mohamed, 2009. A History of Cloud Computing. *Computer Weekly* [online]. TechTarget. [cit. 2015-04-05]. Dostupné z: http://www.computerweekly.com/feature/A-history-of-cloud-computing

BRADSHAW, Simon, Christopher MILLARD a Ian WALDEN, 2010. Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services. *Queen Mary School of Law Legal Studies Research Paper No. 63/2010* [online]. [cit. 2015-04-14]. DOI: http://dx.doi.org/10.2139/ssrn.1662374. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374

BROOKS, Carl, 2010. Amazon's early efforts at cloud computing? Partly accidental: The Troposphere. *TechTarget* [online]. [cit. 2015-04-05]. Dostupné z: http://itknowledgeexchange.techtarget.com/cloud-computing/amazons-early-efforts-at-cloud-computing-partly-accidental/

BUSINESS SOFTWARE ALLIANCE, 2013. *2013 BSA Global Cloud Computing Scorecard: A Clear Path to Progress* [online]. Galexia, 24 s. [cit. 2015-04-07]. Dostupné z: http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf

CATTANEO, Gabriella, Marianne KOLDING, David BRADSHAW a Giuliana FOLCO, 2012. IDC. *Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Up take* [online]. 86 s. [cit. 2015-04-08]. SMART, 2011/0045. Dostupné z: http://cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-report.pdf

CLOUD.CIO.GOV., 2014a. Selecting Services to Move: Cloud.CIO.gov. *Cloud.Cio.Gov: One Stop Source for Federal Cloud Computing Information* [online]. [cit. 2015-03-06]. Dostupné z: http://cloud.cio.gov/topics/selecting-services-move

CLOUD.CIO.GOV., 2014b. Operating within a Cloud Computing Environment: Cloud.CIO.gov. *Cloud.Cio.Gov: One Stop Source for Federal Cloud Computing Information* [online]. [cit. 2015-03-06]. Dostupné z: http://cloud.cio.gov/topics/selecting-services-move

CLOUD.CIO.GOV., 2014c. Cloud Systems: Cloud.CIO.gov. *Cloud.Cio.Gov: One Stop Source for Federal Cloud Computing Information* [online]. [cit. 2015-03-06]. Dostupné z: http://cloud.cio.gov/fedramp/cloud-systems

COTY, Stephen, 2012. *State of Cloud Security Report: An Empirical Analysis of Real World Threats*[online]. Alert Logic [cit. 2015-04-14]. Dostupné z: http://www.alertlogic.com/wp-content/uploads/alert-logic-fall-cloud-security.pdf

CREESE, Guy, 2011. SaaS vs. Software: The Pros and Cons of SaaS Pricing. In: *Gartner Blog Network* [online]. © 2015 [cit. 2015-04-17]. Dostupné z: http://blogs.gartner.com/guy-creese/2010/05/24/saas-vs-software-the-pros-and-cons-of-saas-pricing/

CSA., 2013 *The Notorious Nine: Cloud Computing Top Threats in 2013* [online]. [cit. 2015-04-14]. Dostupné z: http://www.cloudsecurityalliance.org/topthreats

CYRRUS ADVISORY, 2015. Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT (informační a komunikační technologie): Dotace EU. CYRRUS ADVISORY. *Dotace EU: Dotace z EU na klíč* [online]. [cit. 2015-04-08]. Dostupné z: http://www.dotacni.info/zvysovani-efektivity-a-transparentnosti-verejne-spravy-prostrednictvim-rozvoje-vyuziti-a-kvality-systemu-ikt-informacni-a-komunikacni-technologie/

ČERNÝ, Petr a Jana PATTYNOVÁ, 2014. Cloud computing: nová technologie, nové právo?. *Hospodářské Noviny IHNED: Právní rádce* [online]. Praha: Economia, 19. 8. 2014 [cit. 2015-04-14]. Dostupné z: http://pravniradce.ihned.cz/c1-62643550-cloud-computing-nova-technologie-nove-pravo

ČESKÝ STATISTICKÝ ÚŘAD, 2014. IT odborníci v České republice [online]. [cit. 2015-04-14]. Dostupné z: https://www.czso.cz/documents/10180/23188173/it_odbornici_pocty_13.pdf

ČSÚ, 2012. Informační ekonomika v číslech: 2012. ČSÚ. *Český statistický úřad: ČSÚ* [online]. 18.03.2015 [cit. 2015-04-07]. Dostupné z: https://www.czso.cz/csu/czso/informacni-ekonomika-v-cislech-2012-yjc4knxasp

ČSÚ, 2014. Informační technologie ve veřejné správě. Český statistický úřad: ČSÚ [online]. 27.03.2014 [cit. 2015-04-07]. Dostupné z: https://www.czso.cz/csu/czso/informacni-ekonomika-v-cislech-2012-yjc4knxasp

ČTK, 2014. Z části Státní tiskárny cenin vznikne Národní datové centrum. Má státu spravovat IT. *Hospodářské noviny: www.ihned.cz* [online]. Praha: Economia, © 1996-2015 [cit. 2015-04-07]. Dostupné z: http://byznys.ihned.cz/c1-62821460-z-casti-statni-tiskarny-cenin-vznikne-narodni-datove-centrum-ma-statu-spravovat-it

DCOSTA, Amanda, 2012. A Review of PESTLE Analysis History and Application. BRIGHT HUB. [online]. [cit. 2015-04-06]. Dostupné z: http://www.brighthubpm.com/project-planning/100279-pestle-analysis-history-and-application/

DELOITTE, 2014. *Průzkum názorů IT ředitelů: Deloitte CIO Survey 2014* [online]. [cit. 2015-04-08]. Dostupné z: http://www2.deloitte.com/content/dam/Deloitte/cz/Documents/about-deloitte/cz_cio_survey_2014.pdf

ROUSE, Margaret, 2013. What is Hybrid Cloud?: Definition from WhatIs.com. *TechTarget* [online]. [cit. 2015-04-05]. Dostupné z: http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud

E-SCIENCETALK, [2003a]. Grid Computing in 30 Seconds: Gridcafe. *GridCafe* [online].[cit. 2015-04-05]. Dostupné z: http://www.gridcafe.org/EN/grid-in-30-sec.html

E-SCIENCETALK, [2003b]. Five Big Ideas: Gridcafe. *GridCafe* [online].[cit. 2015-04-05]. Dostupné z: http://www.gridcafe.org/EN/five-big-ideas.html

ENISA, 2015. *Security Framework for Governmental Clouds* [online]. [cit. 2015-04-14]. Dostupné z: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/governmental-cloud-security/security-framework-for-govenmental-clouds/security-framework-for-governmental-clouds/at_download/fullReport

ETRO, Federico, 2011. *The Economics of Cloud Computing*. [online]. [cit. 2015-04-14]. Dostupné z:http://www.intertic.org/Policy%20Papers/Report.pdf

ETSI, 2013. *Cloud Standards Coordination: Final Report* [online]. [cit. 2015-04-14]. Dostupné z: http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

EUROCLOUD, © 2010 – 2015. EuroCloud Audit: EuroCloud Slovakia. *EuroCloud Slovakia: Cloud Computing na Slovensku* [online]. [cit. 2015-04-08]. Dostupné z: http://www.eurocloud.sk/category/eurocloud-audit/

EUROPEAN COMMISSION, 2014. Overview on Binding Corporate rules: Justice. European Commission [online]. © 1995-2015 [cit. 2015-04-14]. Dostupné z:http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

EVROPSKÁ KOMISE, 2007. *Zadávání veřejných zakázek v předobchodní fázi: Podpora inovace za účelem zajištění udržitelné vysoké kvality veřejných služeb v Evropě* [online]. Brusel. KOM(2007) 799. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52007DC0799&from=EN

EVROPSKÁ KOMISE, 2010.Rozhodnutí komise ze dne 5. února 2010: o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES. *Úřední věstník Evropské unie* [online]. [cit. 2015-04-14]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:CS:PDF

EVROPSKÁ KOMISE, 2012a. *Uvolnění potenciálu cloud computingu v Evropě*. Brusel. KOM(2012) 529. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52012DC0529&qid=1428280141599&from=CS

EVROPSKÁ KOMISE, 2012b. Stanovisko č. 05/2012 ke cloud computingu [online]. 2012 [cit. 2015-04-14]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_cs.pdf

EVROPSKÁ KOMISE, 2013a. *Digital Agenda: ICT for jobs* [online]. [cit. 2015-04-08]. Dostupné z: http://ec.europa.eu/europe2020/pdf/themes/12_digital_agenda_ict_for_jobs.pdf

EVROPSKÁ KOMISE, 2013b. *Sdělení Komise Evropskému parlamentu a radě: o fungování „bezpečného přístavu" z pohledu občanů EU a společností usazených v EU*. Brusel. KOM(2013) 847. Dostupné z: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282013%290847_/com_com%282013%290847_cs.pdf

EVROPSKÁ KOMISE, 2015a. The Digital Economy and Society Index: DESI. EVROPSKÁ KOMISE. *European Commission* [online]. 24.2.2015 [cit. 2015-04-08]. Dostupné z: http://ec.europa.eu/digital-agenda/en/digital-economy-and-society-index-desi

EVROPSKÁ KOMISE, 2015b. Czech Republic: Digital Agenda for Europe: European Commission. *European Commision* [online]. 24.2.2015 [cit. 2015-04-08]. Dostupné z: ec.europa.eu/digital-agenda/en/scoreboard/czech-republic#1-connectivity

EUROPEAN COMMISSION, 2014a. ICT-08-2015. EUROPEAN COMMISSION. *Research Participant Portal* [online]. 2014, 23.7.2014 [cit. 2015-04-08]. Dostupné z: http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/9081-ict-08-2015.html

EUROPEAN COMMISSION, [2014b]. What is Horizon 2020?: European Commission. *European Commission* [online]. 25.2.2015 [cit. 2015-04-08]. Dostupné z: http://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020

EVROPSKÁ UNIE, 2013. REGULATION (EU) No 1290/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. In: *Official Journal of the European Union*. Strasbourg. Dostupné z: http://ec.europa.eu/research/participants/portal/doc/call/h2020/common/1595113-h2020-rules-participation_oj_en.pdf

FF UK, 2012. *Filozofická fakulta Univerzity Karlovy v Praze* [online]. © 2015 [cit. 2015-04-14]. Dostupné z: http://www.ff.cuni.cz/2012/11/zapis-z-porady-dekana-s-vedoucimi-zakladnich-soucasti-ze-dne-25-rijna-2012/

FF UK, 2014a. *Intranet - SharePoint: Fakultní intranet* [online]. 23. 7. 2014 [cit. 2015-04-14]. Dostupné z: http://manualy.ff.cuni.cz/index.php/Intranet_-_SharePoint

FF UK, 2014b. *Úložiště souborů - OneDrive: OneDrive - úložiště souborů, místo ke sdílení* [online]. 2014, 20. 8. 2014 [cit. 2015-04-14]. Dostupné z: http://manualy.ff.cuni.cz/index.php/Úložiště_souborů_-_OneDrive

FIGLIOLA, Patricia Moloney a Eric A. FISCHER, 2015. *Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management* [online]. Congressional Research Service [cit. 2015-04-06]. Dostupné z: http://www.fas.org/sgp/crs/misc/R42887.pdf

FOSTER, Ian, Yong ZHAO, Ioan RAICU a Shiyong LU, 2008. Cloud Computing and Grid Computing 360-Degree Compared. *2008 Grid Computing Environments Workshop* [online]. IEEE, s. 1-10 [cit. 2015-04-05]. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4738445. DOI: 10.1109/GCE.2008.4738445

FRIESNER, Tim, 2014. History of SWOT Analysis. In: For marketing learners, teachers and professionals.[online]. Marketing Teacher, 2000 - 2015, 8. 5. 2014 [cit. 2015-04-14]. Dostupné z:http://www.marketingteacher.com/history-of-swot-analysis/

GARTNER, 2013. Multitenancy: Gartner IT Glossary. *Technology Research: Gartner Inc.* [online]. Stamford (CT), [cit. 2015-04-05]. Dostupné z: http://www.gartner.com/it-glossary/multitenancy/

GAO, 2014. *CLOUD COMPUTING: Additional Opportunities and Savings Need to Be Pursued: Report to Congressional Requesters* [online]. [cit. 2015-04-17]. Dostupné z:http://www.gao.gov/assets/670/666133.pdf

GHOSH, Shuvanker a Gill HUGHES, 2011. Cloud Computing Explained [online]. [cit. 2015-04-14]. Dostupné z: https://www2.opengroup.org/ogsys/catalog/W115

GOVERNMENT DIGITAL SERVICE, 2014. Sales information: Digital Marketplace. *Welcome to GOV.UK* [online]. [cit. 2015-04-07]. Dostupné z: https://digitalmarketplace.blog.gov.uk/sales-accreditation-information/

HÁJEK, Václav a Štěpán BOJAR, 2014. *Výroční zpráva o činnosti Univerzity Karlovy v Praze za rok 2013*[online]. Praha: Univerzita Karlova [cit. 2015-04-14]. ISBN 978-80-246-2690-1. Dostupné z: https://xs.ruk.cuni.cz/vzc2013/pdf-png/VZC2013reduced.pdf

HARDING, Chris, 2011. *Cloud Computing for Business: The Open Group Guide*. Open Group. ISBN 978-9087536572.

HELLEMANS, Liesbeth, 2014. Legal Implications on Cloud Computing [online]. Cloud For Europe [cit. 2015-04-14]. Dostupné z: http://www.cloudforeurope.eu/news/-/blogs/study-on-the-legal-implications-of-cloud-computing

HERBST, Nikolas Roman, Samuel KOUNEV a Ralf REUSSNER, 2013. Elasticity in Cloud Computing: What It Is, and What It Is Not. In: [online]. [cit. 2014-05-20]. Dostupné z: http://se2.informatik.uni-wuerzburg.de/pa/uploads/papers/paper-209.pdf

HERGESELL, Ondřej, 2014. ICT ve státní a veřejné správě: Český ICT medvěd. *CIO Business World* [online]. IDG Czech Republic, č. 4 [cit. 2015-04-08]. Dostupné z: http://www.ssw.cz/images/_media/files/53736ba6a75d1.pdf

HERZOG, Stephen, 2011. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security* [online]. Henley-Putnam University, vol. 4, no. 2 [cit. 2015-04-14]. Dostupné z: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss

HON, W. Kuan a Christopher MILLARD, 2013. Cloud Technologies and Services. Cloud Computing Law. Ed. Christopher MILLARD. Oxford: Oxford University Press, s. 3-17. ISBN 978-0-19-967167-0

HUGO, Haas a Brown ALLEN, 2004. Web Services Glossary: W3C Working Group Note 11 February 2004. THE WORLD WIDE WEB CONSORTIUM. *World Wide Web Consortium (W3C)* [online]. [cit. 2014-05-20]. Dostupné z: http://www.w3.org/TR/2004/NOTE-ws-gloss-20040211/#webservice

IWGCR, 2014. Downtime Statistics of Current Cloud Solutions: Update version - March 2014. *IWGCR: International Working Group on Cloud Computing Resiliency* [online]. [cit. 2015-04-17].

ISECT, 2015. ISO/IEC 27017 cloud security. *Information Security Standards* [online]. [cit. 2015-04-08]. Dostupné z: http://www.iso27001security.com/html/27017.html

ISO, 2013a. ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements*. ISO/IEC. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO, 2013b. *The ISO Survey of Management System Standard Certifications: 2013* [online]. 2013 [cit. 2015-04-08]. Dostupné z: http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2013

ITU, 2004. *ITU and its Activities Related to Internet-Protocol (IP) Networks* [online]. Geneva: International Telecommunication Union, s. 55-63 [cit. 2015-04-08].

JANSA, Lukáš, 2012. Migrační smlouva v rámci přechodu na Cloud Computing. In: *Právo IT* [online]. © 2009 [cit. 2015-04-14]. Dostupné z: http://www.pravoit.cz/article/migracni-smlouva-v-ramci-prechodu-na-cloud-computing

JISC, 2011. User Guide: Cloud Computing Contracts, SLAs and Terms & Conditions of Use. *JISC legal information: Legal Guidance for ICT Use in Education, Research and External Engagement* [online]. [cit. 2015-04-14]. Dostupné z:http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2141/User-Guide-Cloud-Computing-Contracts-SLAs-and-Terms-Conditions-of-Use-31082011.aspx

KOUBSKÝ, Petr, 2011. ICTU. *Co s veřejnými soutěžemi v ICT: Doporučení k úpravě legislativy a praxe týkající se veřejnýchzakázek v oblasti informačních a telekomunikačních technologií* [online]. Klub ICTU [cit. 2015-04-07]. Dostupné z: http://www.ictu.cz/fileadmin/user_upload/documents/Pozicni_dokumenty/Co_verejnymi_soutezemi_v_ICT_01.pdf

KPMG, 2012. *Exploring the Cloud: A Global Study of Government's Adoption of Cloud* [online]. [cit. 2015-04-17]. Dostupné z: https://www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicaciones/Documents/Exploring-the-Cloud.pdf

KRÁTKÝ, Pavel, 2014. Zákon o kybernetické bezpečnosti v praxi. *IT Systems* [online]. č. 9 [cit. 2015-04-08]. Dostupné z: http://www.systemonline.cz/clanky/zakon-o-kyberneticke-bezpecnosti-v-praxi.htm

KROES, Neelie, 2013. EVROPSKÁ KOMISE. *Statement by Vice President Neelie Kroes: on the consequences of living in an age of total information* [online]. Brussels [cit. 2015-04-08]. Dostupné z: http://europa.eu/rapid/press-release_MEMO-13-654_en.pdf

KUNDRA, Vivek, 2011. *Federal Cloud Computing Strategy* [online]. Washington (DC)[cit. 2015-04-06]. Dostupné z: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

LEACH, Anna, 2013. U.K. Government Looks to Slash ICT Budgets, Improve Service. *Wall Street Journal: Tech Europe* [online]. New York: Dow Jones & Company [cit. 2015-04-07]. Dostupné z: http://blogs.wsj.com/tech-europe/2013/03/14/u-k-government-looks-to-slash-ict-budgets-improve-service/

LEŠTINA, Petr, 2011. Cloud computing versus virtualizace: Rozdíl mezi cloudem a virtualizovaným řešením. *SystemOnLine* [online]. Č. 12 [cit. 2014-05-20]. Dostupné z: http://www.systemonline.cz/virtualizace/cloud-computing-versus-virtualizace.htm. ISSN 1802-615X.

LICHÝ, Alexander, 2014. Jaké byly mzdy IT odborníků v ČR?. *CIO Business World* [online]. IDG Czech Republic [cit. 2015-04-14]. Dostupné z: http://businessworld.cz/kariera/jake-byly-mzdy-it-odborniku-v-cr-11988

LITHNICIUM, David, 2013. As cloud use grows, so will rate of DDoS attacks. In: *InfoWorld* [online]. IDG, © 1994 - 2015 [cit. 2015-04-14]. ISSN 0199-6649. Dostupné z:http://www.infoworld.com/article/2613310/cloud-security/as-cloud-use-grows--so-will-rate-of-ddos-attacks.html

MANAGEMENTMANIA.COM, 2013a. PESTLE analýza. *Sociální síť pro business: ManagementMania.com* [online]. © 2011-2013 [cit. 2015-04-06]. Dostupné z: https://managementmania.com/cs/pestle-analyza

MANAGEMENTMANIA.COM, 2013b. SWOTanalýza. *Sociální síť pro business: ManagementMania.com* [online]. © 2011-2013 [cit. 2015-04-06]. Dostupné z: https://managementmania.com/cs/pestle-analyza

MELL, Peter a Timothy GRANCE, 2011. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *The NIST Definition of Cloud Computing.* [online]. Gaithersburg (Maryland). [cit. 2014-05-20]. Recommendations of the National Institute of Standards and Technology. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

GARTNER, 2005. MIERITZ, Lars a Bill KIRWIN. *Defining Gartner Total Cost of Ownership* [online]. [cit. 2015-04-08]. Dostupné z: http://lib-resources.unimelb.edu.au/gartner/research/131800/131837/131837.pdf

MICROSOFT, © 2015. Licenční smlouva pro řešení ve vzdělávání (EES): Microsoft Školství a vzdělávání. *Školství a vzdělávání* [online]. [cit. 2015-04-14]. Dostupné z: www.microsoft.com/cze/education/licence/ees/

MINISTERSTVO FINANCÍ ČESKÉ REPUBLIKY, 2015. ICT náklady resortů MF, MO, MMR, MŽP, MSp a MD: Otevřená data Ministerstva financí. *Ministerstvo financí ČR* [online]. [cit. 2015-04-08]. Dostupné z: http://data.mfcr.cz/cs/dataset/ict-naklady-resortu-mf-mo-mmr-mzp-msp-md

MF SR, 2012. Centralizáciou dátových centier a prechodom na cloud ušetríme milióny eur. MINISTERSTVO FINANCIÍ SLOVENSKEJ REPUBLIKY. *Ministerstvo financií Slovenskej republiky* [online]. 13.11.2014 [cit. 2015-04-07]. Dostupné z: http://www.mfsr.sk/Default.aspx?CatID=84&NewsID=800

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2011. Klaudie: od správy majetku k modelu poskytování a odebírání služeb. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Efektivní veřejná správa* [online]. © 2015, [cit. 2015-04-07]. Dostupné z: http://www.mvcr.cz/clanek/klaudie-od-spravy-majetku-k-modelu-poskytovani-a-odebirani-sluzeb.aspx

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2015. *STRATEGICKÝ RÁMEC ROZVOJE VEŘEJNÉ SPRÁVY ČESKÉ REPUBLIKY PRO OBDOBÍ 2014 – 2020* [online]. [cit. 2015-04-07]. Dostupné z: http://www.mvcr.cz/odk2/soubor/strategicky-ramec-rozvoje-vs-v-cr-pdf.aspx

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR, [2014]. Fondy EU v ČR: Informace o fondech. *Evropské strukturální a investiční fondy* [online]. Praha [cit. 2015-04-08]. Dostupné z: http://www.strukturalni-fondy.cz/cs/Fondy-EU/Informace-o-fondech-EU

MV ČR, 2012.Strategie 2020: Ministerstvo vnitra České republiky. *Ministerstvo vnitra České republiky* [online]. [cit. 2015-04-06]. Dostupné z: http://www.mvcr.cz/clanek/i2010.aspx

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD, 2015. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*. Praha, 24 s. Dostupné z: https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_cz.pdf

NETMONITOR, 2015. TZ Již 4 miliony uživatelů navštěvují internet z mobilních zařízení. *NetMonitor*[online]. © 2011 [cit. 2015-04-17]. Dostupné z: http://www.netmonitor.cz/tz-jiz-4-miliony-uzivatelu-navstevuji-internet-z-mobilnich-zarizeni

NERV, 2011. *Rámec Strategie konkurenceschopnosti a výchozí náměty NERVu: Závěrečná zpráva podskupin Národní ekonomické rady vlády pro konkurenceschopnost a podporu podnikání* [online]. 1. upr. vyd. Editor Michal Mejstřík. Praha: Úřad vlády České republiky, 307 s. [cit. 2015-04-07]. ISBN 978-80-7440-050-6. Dostupné z: http://www.vlada.cz/assets/ppov/ekonomicka-rada/aktualne/Ramec_strategie_konkurenceschopnosti.pdf

LEIMBACH, Timo, Dara HALLINAN, Daniel BACHLECHNER, Arnd WEBER, Maggie JAGLO, Leonhard HENNEN, Rasmus ØJVIND, Michael NENTWICH, Stefan STRAUß, Theo LYNN, a Graham HUNT, 2014.

Potential and Impacts of Cloud Computing Services and Social Network Websites: Study [online]. [cit. 2015-04-08]. Dostupné z: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET%282014%29513546_EN.pdf

LIU, Fang, Jian MAO, Jin TONG, Robert BOHN, John MESSINA, Lee BADGER a Dawn LEAF, 2011. NIST Special Publication 500 - 292. *NIST Cloud Computing Reference Architecture*. Gaithersburg (MD): National Institute of Standards and Technology. Dostupné z: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

MILLER, Rich, 2010. Kundra: Fed Data Centers 7 Percent Utilized. In: *Data Center Knowledge: Industry News and Analysis About Datacentres* [online]. iNET Interactive, © 2015 [cit. 2015-04-14]. Dostupné z: http://www.datacenterknowledge.com/archives/2010/04/09/kundra-fed-data-centers-7-percent-utilized/

HAMDAQA, Mohammad; Ladan, TAHVILDARI, 2012. Cloud computing uncovered: a research landscape. *Advances in Computers*, 86: 41-85. Dostupné z: http://www.stargroup.uwaterloo.ca/~mhamdaqa/publications/Cloud_Computing_Uncovered.pdf.

HASHEMI, Seyyed Mohsen a Amid Khatibi BARDSIRI, 2012. Cloud Computing Vs. Grid Computing. *ARPN Journal of Systems and Software* [online]. Roč. 2, č. 5 [cit. 2015-04-05]. Dostupné z: http://scientific-journals.org/journalofsystemsandsoftware/archive/vol2no5/vol2no5_4.pdf.

HAUGER, Doug, 2010. Windows Azure General Availability. In: *The Official Microsoft Blog* [online]. Microsoft, © 2015 [cit. 2015-04-14]. Dostupné z:http://blogs.microsoft.com/blog/2010/02/01/windows-azure-general-availability/

MICROSOFT, 2015a. Microsoft Licensing Solution Partners: LSP. *Microsoft Partner Network Home*[online]. [cit. 2015-04-14]. Dostupné z: https://mspartner.microsoft.com/cs/cz/Pages/Community/microsoft-large-account-reseller.aspx

NETO, Maximilliano Destefani, 2014. A brief history of cloud computing. *Thoughts on Cloud* [online]. [cit. 2015-04-05]. Dostupné z: http://www.thoughtsoncloud.com/2014/03/a-brief-history-of-cloud-computing/

PATTYNOVÁ, Jana, 2012. Cloud Computing a veřejné zakázky. *Egovernment: elektronizace verejne spravy* [online]. č. 12 [cit. 2015-04-14]. Dostupné z:http://www.egovernment.cz/archiv/PDF%202-12/16.pdf

PAVLÁT, David, 2013. K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb.Věstník Úřadu pro ochranu osobních údajů [online]. Úřad pro ochranu osobních údajů [cit. 2015-04-14]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002

PETERKA, Jiří. ICTU, 2012a. *Sdílení ICT služeb ve veřejné správě: Návrh vybraných opatření pro snížení rozpočtových nákladů v době ztížených ekonomických podmínek* [online]. Klub ICTU [cit. 2015-04-08]. Dostupné z: http://www.ictu.cz/fileadmin/user_upload/documents/Pozicni_dokumenty/ICTU_Sdileni_ICT_sluzeb.pdf

PETERKA, Jiří, 2012b. Quo vadis, KIVS?. *Lupa.cz: server o českém Internetu* [online]. © 1998 – 2015 [cit. 2015-04-08]. Dostupné z: http://www.lupa.cz/clanky/quo-vadis-kivs/

PETRŮJ, Jan. Veřejná správa se musí „mobilizovat". In: *E15: Euro* [online]. Mladá fronta, 2015 [cit. 2015-04-17]. Dostupné z: http://euro.e15.cz/archiv/verejna-sprava-se-musi-mobilizovat-1052242#utm_medium=selfpromo&utm_source=e15&utm_campaign=copylink

POKORNÝ, Ondřej a Miroslav KOSTIĆ, 2013. *Možnosti implementace programu na zadávání veřejných zakázek v předobchodní fázi* [online]. Praha: Technologické centrum AV ČR, 54 s. [cit. 2015-04-08]. Dostupné z: http://www.vyzkum.cz/storage/att/39215D8989628142C1E6B779600FF5B8/Implemantace_SBIR_2013.pdf

RAPPA, Michael A, 2004. The utility business model and the future of computing services. *IBM Systems Journal*. Roč. 43, č. 1. Dostupné z: http://cs.nju.edu.cn/yangxc/utility-computing/rappa.pdf. ISSN 0018-8670.

READING, Viviane, 2009. Digital Europe: Europe's Fast Track to Economic Recovery. In: *The Ludwig Erhard Lecture 2009* [online]. Brussels [cit. 2015-04-06]. Dostupné z: http://europa.eu/rapid/press-release_SPEECH-09-336_en.pdf

SERVODATA, 2013. *Priloha 2 - nabidka: Krycí list nabídky: Softwarové licence a související služby pro osobní počítače a servery*. Dostupné z: http://sluzby.e-zakazky.cz/Profil-Zadavatele/ad68556a-1413-446a-844e-fbeb3ba226db/Zakazka/P13V00000007

SCHOFIELD, Jack, 2011. John McCarthy obituary. *The guardian* [online]. [cit. 2015-04-05]. Dostupné z: http://www.theguardian.com/technology/2011/oct/25/john-mccarthy. ISSN 0261-3077.

SCHMIDT, Eric. Search Engine Strategies Conference: Conversation with Eric Schmidt hosted by Danny Sullivan. GOOGLE, Inc. *Google: Press Center* [online]. Mountain View (CA), 2006 [cit. 2015-04-05]. Dostupné z: http://www.google.com/press/podium/ses2006.html

STEHLÍK, Michal, 2012. *Aktualizace Dlouhodobého záměru FF UK: pro akademický rok 2012/2013*[online]. [cit. 2015-04-14]. Dostupné z: http://www.ff.cuni.cz/FF-122-version1-Aktualizace_DZ_FFUK_2012_13.pdf

STRICKLAND, Jonathan, 2008. How Grid Computing Works. *HowStuffWorks* [online]. Blucora [cit. 2015-04-05]. Dostupné z: http://computer.howstuffworks.com/grid-computing.htm

STROUHAL, Jaroslav, 2014. *Návrh opatření zvyšujících efektivnost služeb veřejné správy a podpůrných ICT služeb*. [cit. 2015-04-07]. Dostupné z: http://www.ospzv-aso.cz/addons/112%20RHSD/Navrh-opatreni-zvysujicich-efektivnost-sluzeb-verejne-spravy-a-podpurnych-ICT-suzeb.pdf

TECHNOLOGICKÁ AGENTURA ČR, 2014. Premiéra ve státní správě: první vyhlášení veřejné zakázky metodou PCP v ČR. *TAČR: Technologická agentura ČR* [online]. © 2015, 7. 3. 2014 [cit. 2015-04-08]. Dostupné z: www.tacr.cz/index.php/cz/novinky/291-premiera-ve-statni-sprave-prvni-vyhlaseni-verejne-zakazky-metodou-pcp-v-cr.html

Tichý, Ondřej, 2015. Re: RE: Implementace Office 365 na FF UK - zadost o zodpovezeni otazek pro diplomovou praci [online]. Message to: Tomáš Rejnek. 9. 4. 2015 [cit. 2015-04-14].

URBAN, Jakub, 2012. Není SharePoint jako SharePoint. In: *Živě.cz* [online]. Mladá fronta, 2015 [cit. 2015-04-14]. ISSN 1212-8554. Dostupné z: http://www.zive.cz/clanky/neni-sharepoint-jako-sharepoint/sc-3-a-163574

VAQUERO, Luis M., Luis RODER-MERINO, Juan CACERES a Lindner MAIK. A break in the clouds: towards a cloud definition. *ACM SIGCOMM: Computer Communication Review* [online]. 2009, roč. 39, č. 1, s. 50-55 [cit. 2014-05-20]. Dostupné z: https://research.ibm.com/haifa/projects/systech/reservoir/public/CloudDefinitionPaper.pdf. DOI: 10.1145/1496091.1496100.

VERGE, Jason, 2014. Google Buys More Swedish Wind Power For Its Finnish Data Center. In: *Data Center Knowledge: Industry News and Analysis About Datacentres* [online]. iNET Interactive, © 2015 [cit. 2015-04-14]. Dostupné z: http://www.datacenterknowledge.com/archives/2014/01/23/google-buys-swedish-wind-power-finnish-data-center/

VERIZON, 2014. *2014 DATA BREACH INVESTIGATIONS REPORT* [online]. [cit. 2015-04-14]. Dostupné z: http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf

VLÁDA ČESKÉ REPUBLIKY, 2013. *Digitální Česko v. 2.0: Cesta k digitální ekonomice* [online]. Praha [cit. 2015-04-07]. Dostupné z: http://www.vlada.cz/assets/media-centrum/aktualne/Digitalni-Cesko-v--2-0_120320.pdf

VOLF, Tomáš, 2012. Firmy v Česku míří na cloud. Průkopníky jsou T-Mobile, ČEZ nebo Poštovní spořitelna. *Hospodářské noviny: ihned.cz* [online]. [cit. 2015-04-05]. Dostupné z: http://byznys.ihned.cz/c1-54707920-firmy-v-cesku-miri-na-cloud-prukopniky-jsou-t-mobile-cez-nebo-postovni-sporitelna

VOJKOVSKÝ, Jiří, 2013. Kdo je to cloud broker: a jaký smysl mají jeho služby?. In: *IT SYSTEMS* [online]. © 2001 - 2015 [cit. 2015-04-14]. ISSN 1802-615X. Dostupné z:http://www.systemonline.cz/virtualizace/kdo-je-to-cloud-broker.htm

Evropská komise. Sdělení komise. Evropa 2020: Strategie pro inteligentní a udržitelný růst podporující začlenění [online]. Brusel, 2010a [cit. 2013 11 10]. Dostupné z WWW: